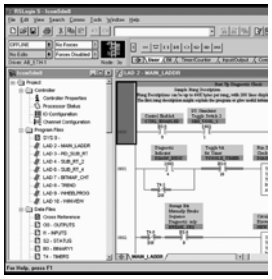
Stratix 8000 and Stratix 8300 Ethernet Managed Switches



User Manual

Catalog Numbers 1783-MS06T, 1783-MS10T, 1783-RMS06T, 1783-RMS10T, 1783-MX08T, 1783-MX08F

ALLEN-BRADLEY • ROCKWELL SOFTWARE

Rockwell Automation

Important User Information

Solid state equipment has operational characteristics differing from those of electromechanical equipment. Safety Guidelines for the Application, Installation and Maintenance of Solid State Controls (publication SGI-1.1 available from your local Rockwell Automation sales office or online at http://www.rockwellautomation.com/literature) describes some important differences between solid state equipment and hard-wired electromechanical devices. Because of this difference, and also because of the wide variety of uses for solid state equipment, all persons responsible for applying this equipment must satisfy themselves that each intended application of this equipment is acceptable.

In no event will Rockwell Automation, Inc. be responsible or liable for indirect or consequential damages resulting from the use or application of this equipment.

The examples and diagrams in this manual are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular installation, Rockwell Automation, Inc. cannot assume responsibility or liability for actual use based on the examples and diagrams.

No patent liability is assumed by Rockwell Automation, Inc. with respect to use of information, circuits, equipment, or software described in this manual.

Reproduction of the contents of this manual, in whole or in part, without written permission of Rockwell Automation, Inc., is prohibited.

Throughout this manual, when necessary, we use notes to make you aware of safety considerations.

WARNING	Identifies information about practices or circumstances that can cause an explosion in a hazardous environment, which may lead to personal injury or death, property damage, or economic loss.
IMPORTANT	Identifies information that is critical for successful application and understanding of the product.
ATTENTION	Identifies information about practices or circumstances that can lead to personal injury or death, property damage, or economic loss. Attentions help you identify a hazard, avoid a hazard, and recognize the consequence
SHOCK HAZARD	Labels may be on or inside the equipment, for example, a drive or motor, to alert people that dangerous voltage may be present.
BURN HAZARD	Labels may be on or inside the equipment, for example, a drive or motor, to alert people that surfaces may reach dangerous temperatures.

Allen-Bradley, Rockwell Automation, Rockwell Software, RSLinx, RSLogix 5000, Stratix 8000, Stratix 8300, and TechConnect are trademarks of Rockwell Automation, Inc.

Trademarks not belonging to Rockwell Automation are property of their respective companies.

What Changed

This information changed or was added since the last revision of this manual. These changes are associated with revision 4 of the Stratix 8000 and Stratix 8300 Ethernet Managed Switches.

Updates include the following:

- Addition of the Stratix 8300 Ethernet Managed Switch
- Addition of the IP routing feature to the Stratix 8300 Ethernet Managed Switch

Revision bars indicate changes made since the last revision.

Notes:

Summary of Changes What Changed . . . 3

Table of Contents

Preface
About This Publication . . . 9
Who Should Use This Publication . . . 9
Additional Resources . . . 10

Chapter 1

Getting Started
Introduction . . . 11
Stratix 8000 and Stratix 8300 Ethernet Managed Switches . . . 12
Hardware Features . . . 15
CompactFlash Memory Card . . . 16
Switch Memory Allocation . . . 17
Initialize the Switch with Express Setup . . . 17
Device Manager Web Interface . . . 22
- Hardware Requirements . . . 23
- Software Requirements . . . 23

RSLogix 5000 Software Interface . . . 23
- Hardware Requirements . . . 24
- Software Requirements . . . 24

Cisco Network Assistant . . . 25
Command Line Interface . . . 26

Chapter 2

Switch Software Features
Introduction . . . 27
Port Numbering . . . 27
Global Macro . . . 29
Smartports . . . 29
- Optimize Ports through Smartports Port Roles . . . 29
- Avoid Smartports Mismatches . . . 31

VLANs . . . 31
- Isolate Traffic and Users . . . 32
- Isolate Different Traffic Types . . . 33
- Group Users . . . 34

IGMP Snooping With Querier . . . 34
Spanning Tree Protocol . . . 35
- Rapid Spanning Tree Protocol . . . 36

Storm Control . . . 36
- Default Storm Control Configuration . . . 38

Port Security . . . 38
- Dynamic Secure MAC Address (MAC ID) . . . 38
- Static Secure MAC Address (MAC ID) . . . 39
- Security Violations . . . 39

EtherChannels . . . 40
DHCP Persistence . . . 41
Precision Time Protocol (PTP) . . . 42
Resilient Ethernet Protocol (REP) . . . 42

REP Open Segment. 43
REP Ring Segment 44
Access Ring Topologies. 45
Link Integrity 46
SNMP 46
Supported MIBs. 48
Port Mirroring 49
Layer 3 Routing (Stratix 8300 Switch Only) 50
Types of Routing 51
Alarms. 52
Cryptographic IOS Software 52
Advanced Software Features 53

Chapter 3

Manage the Switch via the Device Manager Web Interface

Introduction 55
Access the Device Manager Web Interface 56
Front Panel View and Status Indicators 57
Status Field. 61
Assign Port Roles. 62
Customize Port Role Attributes 63
Update Port Settings 63
Update Switch IP Information 66
Configure VLANs 69
Assign Ports to VLANs. 70
Advanced VLAN Configuration. 71
Configure SNMP 72
Configure EtherChannels 75
Configure DHCP Persistence 76
Set up the DHCP Server 77
Configure a DHCP IP Address Pool 78
Reserve IP Addresses through DHCP Persistence 80
Synchronize the Switch with Other Devices via PTP 83
Set the Synchronization Clock Mode 84
Change the PTP Timing Message Settings. 85
Configure REP Segments 88
Configure IP Addresses. 91
Assign IP Addresses to VLANs 91
Enable Static Routing
(Stratix 8300 Switches Only) 91
Route Across VLANs 91
Route Across Ports 92
Configure Port Mirroring. 93
Dashboard Dialog Box 93
Switch Information 95
Bandwidth Used Gauge. 95
Packet Error Gauge. 96

Temperature Status 97
Port Utilization and Port Errors Graphs 97
Trends Graphs 98
Port Status 100
Port Statistics 101
Alert Log 102
CIP Status 104
Upgrade the Switch Firmware 106

Chapter 4

Manage the Switch via RSLogix 5000 Software

Introduction 109
EtherNet/IP CIP Interface 109
CIP Network Connections 110
RSLinx Software and Network Who Support 111
Electronic Data Sheet (EDS) Files 111
Data Accessible With CIP 112
Add a Switch to the I/O Configuration Tree 114
Configure Module Properties 116
Connection Properties 119
General Switch Properties 120
Basic Port Properties 122
Advanced Port Properties 124
Port Thresholds (Storm Control) 128
Save and Restore Switch Configuration 130
Monitor and Reset the Switch 131
Switch Status 133
Port Status 135

Chapter 5

Troubleshoot the Switch

Introduction 141
Run a Diagnostic Test 141
IP Address Issues 143
Device Manager Issues 144
Switch Performance 144
Access Direct Managed Mode 146
Restart or Reset the Switch 147
Restart the Switch from the Device Manager Web Interface . . . 148
Restart the Switch from RSLogix 5000 Programming Software . 148
Reset the Switch to Factory Defaults 148
Recover the Switch Firmware and Restore Factory Defaults 149
Troubleshoot a Firmware Upgrade 150

Appendix A

I/O Data Types

Appendix B

Port Assignments for CIP Data

Appendix C

Cables and Connectors

10/100 and 10/100/1000 Ports 159
Connect to 10BASE-T- and 100BASE-TX-Compatible Devices . . . 160
100BASE-FX Ports 162
SFP Module Ports 162
Dual-purpose Ports 163
Console Port 163
Cable and Adapter Specifications 164
SFP Module Cable Specifications 164
Adapter Pinouts 164

Index

About This Publication

This publication describes the embedded software features and tools for configuring and managing the Stratix 8000 Ethernet Managed Switch with the RSLogix 5000 software Add-on Profile (AOP), or the Device Manager Web interface. In addition, this publication provides troubleshooting information to help you resolve basic switch and network issues.

For information on additional software features, or further configuration of these features, see the Cisco publications listed on page 10.

Who Should Use This Publication

This guide is for the person configuring and monitoring Stratix 8000 Ethernet Managed Switches. We assume that you are familiar with these topics:

- Local-area network (LAN) switch fundamentals
- Concepts and terminology of the Ethernet protocol and local area networking

Additional Resources

These documents contain additional information concerning this Rockwell Automation product.

Resource	Description
Stratix 8000 Ethernet Managed Switches Installation Instructions, publication 1783-IN005	Describes how to get started installing and configuring the switch.
Stratix 8000 Ethernet Managed Switches Release Notes, publication 1783-RN002	Lists enhancements and anomalies associated with the released software version.
Device Manager Web interface online help (provided with the switch)	Provides context-sensitive information on configuring and using the switch, including system messages.
Industrial Automation Wiring and Grounding Guidelines, publication 1770-4.1	Provides general guidelines for installing a Rockwell Automation industrial system.
Product Certifications website, http://www.ab.com	Provides declarations of conformity, certificates, and other certification details.

You can view or download publications at http://www.rockwellautomation.com/literature. To order paper copies of technical documentation, contact your local Rockwell Automation distributor or sales representative.

Other manuals that may be of use to you are available at http://www.Cisco.com.

These include:

- Cisco IE-3000 Command Line Reference Manual
- Cisco IE-3000 Software Configuration Guide
- Cisco IE-3000 Switch System Message Guide

Getting Started

Introduction

The Stratix 8000 and Stratix 8300 Ethernet Managed Switches provide a secure switching infrastructure for harsh environments. You can connect these switches to network devices such as servers, routers, and other switches. In industrial environments you can connect Ethernet-enabled industrial communication devices including programmable logic controllers (PLCs), human-machine interfaces (HMIs), drives, sensors, and I/O.

The Stratix 8000 Ethernet Managed Switch is a Layer 2 switch. The Stratix 8300 Ethernet Managed Switch adds Layer 3 routing to the Stratix 8000 switch The Stratix 8300 switch contains all the features of the Stratix 8000 switch, plus a number of IP routing protocols, along with enhanced security and QoS features.

Topic	Page
Stratix 8000 and Stratix 8300 Ethernet Managed Switches	12
Hardware Features	15
CompactFlash Memory Card	17
Switch Memory Allocation	17
Initialize the Switch with Express Setup	17
Device Manager Web Interface	22
RSLogix 5000 Software Interface	23
Cisco Network Assistant	25
Command Line Interface	26

Stratix 8000 and Stratix 8300 Ethernet Managed Switches

The following table lists available switches, expansion modules, and SFP modules.

Cat. No.	Description
Stratix 8000 Switches (Layer 2)	
1783-MS06T	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot.
1783-MS10T	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot.
Stratix 8300 Switch (Layer 3)	
1783-RMS06T	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot.
1783-RMS10T	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot.
Expansion Modules	
1783-MX08T	Expansion module with 8 10/100BASE-T copper Ethernet ports
1783-MX08F	Expansion module with 8 100BASE-FX fiber optic Ethernet ports
SFP Modules	
1783-SFP100FX	100BASE-FX 100 M multi-mode fiber transceiver
1783-SFP1GSX	1000BASE-SX 1 G multi-mode fiber transceiver
1783-SFP100LX	100BASE-LX 100 M single-mode fiber transceiver
1783-SFP1GLX	1000BASE-LX 1 G single-mode fiber transceiver

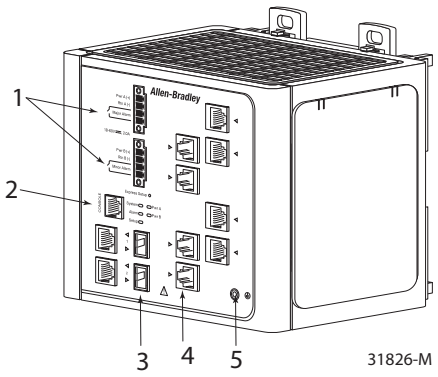
Cat. No.	Description
1606-XL series (recommended) 1606-XLP series (recommended) Or equivalent	Class 2, 24V DC output power supplies

Cat. No.	Description
1783-MCF	Stratix 8000 CompactFlash card (spare)
1783-RMCF	Stratix 8300 CompactFlash card (spare)

Cat. No.	Description
1783-MCS	Stratix 8000 Cryptographic IOS Software
1783-RMCS	Stratix 8300 Cryptographic IOS Software

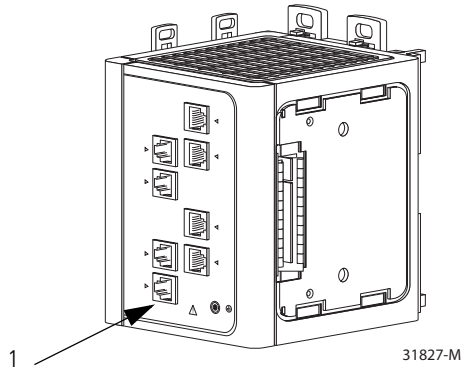
The switch front panel contains the ports, the status indicators, and the power and relay connectors. The following figures show the 1783-MS10T switch and expansion module front panels.

1783-MS10T Switch



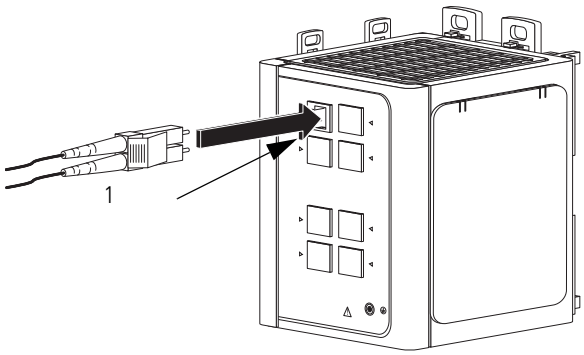
1 Power and relay connectors
2 Console port
3 Dual-purpose ports
4 10/100 ports
5 Protective ground connection

1783-MX08T Switch Copper Expansion Module (side cover removed)



1 10/100 ports

1783-MX08F Switch Fiber Expansion Module



31797-M

1 100BASE-FX ports

Hardware Features

These features are common to both the Stratix 8000 and Stratix 8300 switches. See the figures on pages 13…14 for an illustration of these features.

Feature	Description
Power and relay connector	You connect the DC power and alarm signals to the switch through two front panel connectors. One connector provides primary DC power (supply A) and the major alarm signal, and a second connector (supply B) provides secondary power and the minor alarm signal. The two connectors are physically identical and are in the upper left side of the front panel. The switch can operate with a single power source or with dual power sources. When both power sources are operational, the switch draws power from the DC source with the higher voltage. If one of the two power sources fail, the other continues to power the switch. The power and relay connectors also provide an interface for two independent alarm relays: the major alarm and the minor alarm. The relays can be activated for environmental, power supply, and port status alarm conditions and can be configured to indicate an alarm with either open or closed contacts. The relay itself is normally open, so under power failure conditions, the contacts are open. From the Command Line Interface (CLI), you can associate any alarm condition with one alarm relay or with both relays.
Console port	For configuring, monitoring, and managing the switch, you can connect a switch to a computer through the console port and the supplied RJ45-to-DB-9 adapter cable. If you want to connect a switch to a terminal, you need to provide an RJ45-to-DB-25 female DTE adapter.
Dual-purpose uplink ports	The two dual-purpose uplink ports may each be configured for RJ45 (copper) or SFP (fiber) media types. Only one of these connections in each of the dual-purpose ports can be active at a time. If both ports are connected, the SFP module port has priority. You can set the copper RJ45 ports to operate at 10, 100, or 1000 Mbps in full-duplex or half-duplex mode. You can configure them as fixed 10, 100, or 1000 Mbps (Gigabit) Ethernet ports and can configure the duplex setting. You can use approved Gigabit (or 100 Mbps) Ethernet SFP modules to establish fiber-optic connections to other switches. These transceiver modules are field-replaceable, providing the uplink interfaces when inserted in an SFP module slot. You use fiber-optic cables with LC connectors to connect to a fiber-optic SFP module. These ports operate in the full-duplex mode only.
10/100 ports	You can set the 10/100 ports to operate at 10 or 100 MbpsMbps in full-duplex or half-duplex mode. You can also set these ports for speed and duplex autonegotiation in compliance with IEEE 802.3-2002. (The default setting is autonegotiate.) When set for autonegotiation, the port senses the speed and duplex settings of the attached device. If the connected device also supports autonegotiation, the switch port negotiates the best connection (that is, the fastest line speed that both devices support and full-duplex transmission if the attached device supports it) and configures itself accordingly. In all cases, the attached device must be within 100 m (328 ft) of the switch.

Feature	Description
100BASE-FX ports	The IEEE 802.3-2002 100BASE-FX ports (on the 1783-MX08F expansion module) provide full-duplex 100 Mbps connectivity over multimode fiber (MMF) cables. These ports use a built-in, small-form-factor fixed (SFF) fiber-optic transceiver module that accepts a dual LC connector. The cable can be up to 2 km (1.24 mi.) in length.
Rear panel	The rear panels of the switches and expansion modules have latches for installation on either a DIN rail or a wall. The latches slide outward to position the switch over the DIN rail and slide inward to secure the switch to a DIN rail. The feet must be extended when mounting the switch on heavy-duty (35 x 15 mm) DIN rail or they may be extended for improved ventilation when wall mounting.
Auto-MDIX	When connecting the switch to workstations, servers, and routers, straight-through cables are normally used. However, the automatic medium-dependent interface crossover (auto-MDIX) feature of the switch is enabled by default and will automatically re-configure the ports to use either straight-through or crossover cable type. The Auto-MDIX feature is enabled by default. When the auto-MDIX feature is enabled, the switch detects the required cable type (straight-through or crossover) for copper Ethernet connections and configures the interfaces accordingly. You can use the command-line interface (CLI) to disable the auto-MDIX feature. See the online help for more information.

CompactFlash Memory Card

The CompactFlash card contains the switch IOS operating system, the Device Manager Web interface firmware and the user switch configuration. Without the CompactFlash card installed the switch cannot complete powerup or restart).

If the card is removed with the switch running, the switch will continue to function; however, the Device Manager Web interface will no longer be available.

If any changes are made to the switch configuration after the card is removed (via the CLI or CIP interface), they will be applied and used by the switch (running configuration); however, the changes will not be saved.

If the CompactFlash card is inserted sometime later, the changes will not be saved to the card unless new changes are made. Each time a change is made with the card installed, both the AOP and the Device Manager Web interface save the entire running configuration to the card.

Switch Memory Allocation

The following table provides details on default memory allocation for the Stratix 8000 and Stratix 8300 switches. You can modify the amount of memory allocated by using different allocation templates with the command line interface (CLI).

Feature	Stratix 8000 Switch	Stratix 8300 Switch
Unicast MAC addresses	8 K	2 K
IPv4 IGMP groups + multicast routes	0.25 K	1 K
IPv4 unicast routes	-	4 K
Directly connected IPv4 hosts	-	2 K
Indirect IPv4 routes	-	2 K
IPv4 policy based routing aces	-	0.5 K
IPv4/MAC QoS aces	0.375 K	0.625 K
IPv4/MAC security aces	0.375 K	0.375 K

Initialize the Switch with Express Setup

The switch can operate without an IP address assigned to it. However, without an IP address, your switch will run as an unmanaged switch, and is limited to using only the status indicators on the switch front panel for diagnostics. We recommend that you run the Express Setup program to enter the switch initial IP information.

1. While the Setup status indicator flashes green, start an Internet browser session on the personal computer.

   The switch prompts you for the default switch username and password.

2. Leave the username field blank.

3. Enter the default switch password, ‘switch’.

   The Express Setup dialog box automatically appears.

4. If the window does not appear, do the following:
   - enter the URL of a well-known website in your browser to be sure the browser is working correctly.

     Your browser will then automatically be directed to the Express Setup Web page.

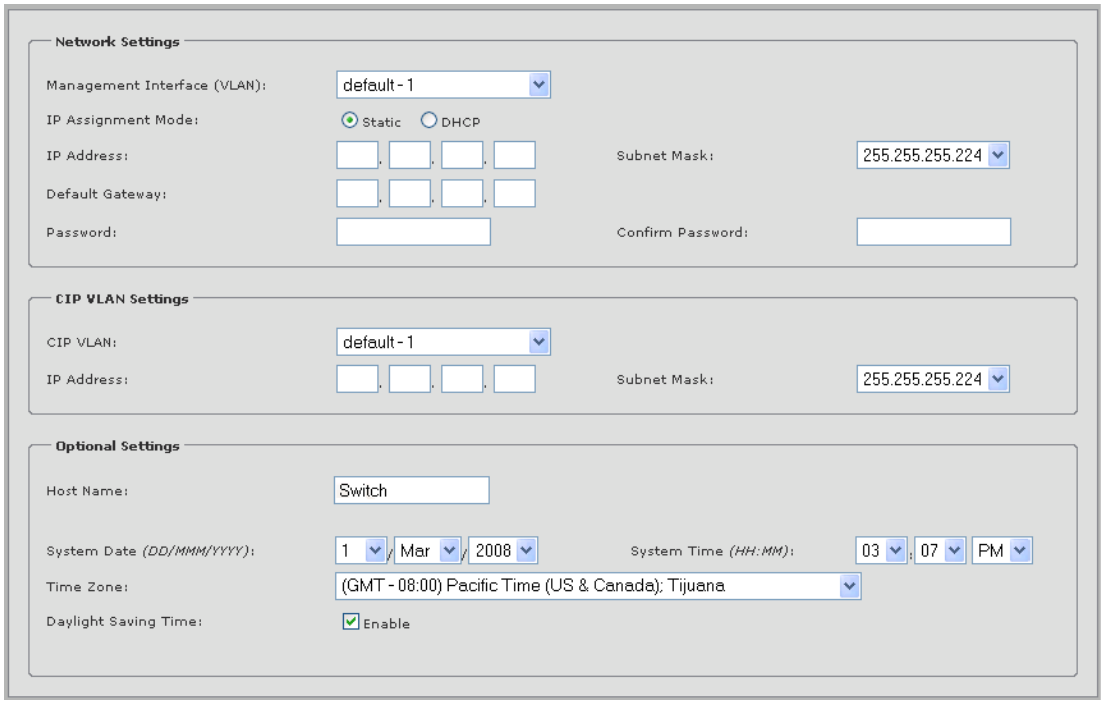
   - verify that any proxy settings or pop-up blockers are disabled on your browser.

- verify that any wireless interface is disabled on your personal computer..

TIP You may also enter the URL http://169.254.0.1/express-setup.htm to access the Express Setup page directly.

- Enter the network settings.

All entries must be English letters and Arabic numbers.



Network Settings	Description
Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch will be managed. Select an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1…1001. Make sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should be limited to a specific group of users (such as the administrators of your network). It also ensures secure administrative access to all devices in the network at all times. Refer to VLANs on page 31 for more information about management VLANs and about VLANs in general.
IP Assignment Mode	The IP Assignment mode determines if the switch IP information is manually assigned (Static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you select Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you select DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, make sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server will automatically assign to other devices. This prevents IP-address conflicts between the switch and another device.
IP Address	The IP address is a unique identifier for the switch in a network. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same. You cannot assign the switch with an IP address in the 10.0.0.0 network.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static.

Network Settings	Description
Default Gateway	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address should be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP Assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate.
Password	You must provide a password to the switch to secure the access to the Device Manager Web interface. This password is also used as the Control and Information Protocol (CIP) security password. Change the password from the default password, 'switch'. The password you choose for the switch follows these guidelines: • Can have up to 63 alphanumeric characters • Can start with a number • Is case sensitive • Can have embedded spaces • Cannot be a single digit • Cannot contain a ? or a tab • Does not allow spaces at the beginning or the end
Confirm Password	Enter the switch password again.

Setting	Description
CIP VLAN	The VLAN on which CIP will be enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on the switch. The default ID is 1. The default name for the CIP VLAN is default.
IP Address	The IP address is a unique identifier for the switch in a network. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0...255. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. If the CIP VLAN is different from the management VLAN, you must specify a subnet mask for the CIP VLAN.

5. Enter the optional settings now, or enter them later by using the Device Manager Web interface.

Optional Setting	Description
Host Name	A name for the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ?, a space, or a tab. The default is 'switch'. We recommend entering either the name, the location, or the IP address of the switch to help identify the switch during monitoring or troubleshooting.
System Date	The date that the switch read from the network management station or that was manually set during the initial setup. If you change the date, the change takes effect immediately after you click Submit.
System Time	The time that the switch read from the network management station or that was manually set during the initial setup. If you change the time, the change takes effect immediately after you click Submit.

TIP For more information about the optional settings, from the toolbar, click Help.

6. Click Submit to save the information that you entered and to finish the basic configuration.
   - Once you click Submit, the switch initializes its configuration for typical industrial EtherNet/IP applications.

     The switch then redirects you to the Device Manager Web interface logon pages. From here, you can continue to launch the Device Manager Web interface for further configuration, or exit.

- If you click Cancel, the fields are cleared, and you can start over.

7. Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network.

8. After you complete Express Setup, refresh the personal computer IP address.
   - For a dynamically-assigned IP address, disconnect the personal computer from the switch, and reconnect the personal computer to the network. The network DHCP server assigns a new IP address to the personal computer.
   - For a statically-assigned IP address, change it to the previously configured IP address.

Device Manager Web Interface

You can manage the switch by using the Device Manager Web interface to configure and monitor the switch. The Device Manager Web interface is a graphical device management tool for configuring, monitoring, and troubleshooting individual switches.

The Device Manager Web interface displays real-time views of switch configuration and performance. It simplifies configuration tasks with features such as Smartports to quickly set up the switch and its ports. It uses graphical, color-coded displays, such as the Front Panel view, graphs, and animated indicators to simplify monitoring tasks. It provides alert tools to help you to identify and to solve networking problems.

You can display the Device Manager Web interface from anywhere in your network through a Web browser such as Microsoft Internet Explorer.

Hardware Requirements

Attribute	Requirement
Processor speed	233 MHz min 1 GHz recommended
RAM	512 MB min 1 GB recommended
Free hard drive space	50 MB
Number of colors	256
Resolution	1024 x 768
Font size	Small

Software Requirements

Operating System	Microsoft Internet Explorer	Mozilla Firefox
Windows 2000	6.0, 7.0	1.5, 2.0
Windows 2003	6.0, 7.0	1.5, 2.0
Windows Vista	6.0, 7.0	1.5, 2.0
Windows XP	6.0, 7.0	1.5, 2.0

The Device Manager Web interface verifies the browser version when starting a session to ensure that the browser is supported.

TIP So that the Device Manager Web interface runs properly, disable any pop-up blockers or proxy settings in your browser software and any wireless client s running on your computer or laptop.

RSLogix 5000 Software Interface

You can manage the switch by using the RSLogix 5000 software to configure and monitor the switch. RSLogix 5000 software is an IEC 61131-3 compliant software package that offers relay ladder, structured text, function block diagram, and sequential function chart editors for you to develop application programs.

Hardware Requirements

Attribute	Requirement
Processor speed	Pentium II 450 MHz min Pentium III 733 MHz (or better) recommended
RAM	128 MB min 256 MB recommended
Free hard drive space	3 GB
Optical drives	DVD
Video requirements	256-color VGA graphics adapter 800 x 600 min resolution (True Color 1024 x 768 recommended)
Resolution	800 x 600 min resolution (True Color 1024 x 768 recommended)

Software Requirements

Attribute	Requirements
Supported operating systems	RSLogix 5000 software, version 17 has been tested on the following operating systems: • Microsoft Windows XP Professional with Service Pack 2 • Microsoft Windows Server 2003 R2 Standard Edition with Service Pack 1 and User Account Control (UAC) turned off • Microsoft Windows 2000 Professional with Service Pack 4 • Microsoft Windows Vista Home Basic with SPI • Microsoft Windows Vista Business with SPI RSLogix 5000 software is expected to operate correctly on the following operating systems, but has not been tested: • Microsoft • Microsoft Windows XP Home • Microsoft Windows Server 2003 Standard Edition with Service Pack 1 • Microsoft Windows 2000 Professional with Service Pack 1, 2, or 3 • Microsoft Windows Vista Ultimate • Microsoft Windows Vista Home Premium The Chinese, Japanese, and Korean editions of RSLogix 5000 software are supported only on Microsoft Windows XP, Microsoft Windows Vista, and Microsoft Windows Server 2003. RSLogix 5000 software is supported for 32-bit architectures (x86) and has not been tested with 64-bit architectures (x64).

Cisco Network Assistant

Cisco Network Assistant is a Web interface that you download from Cisco's website and run on your computer. It offers advanced options for configuring and monitoring multiple devices, including switches, switch clusters, switch stacks, routers, and access points.

Follow these steps to use the software.

1. Go to http://www.cisco.com/go/NetworkAssistant.

   You must be a registered user, but you need no other access privileges.

2. Find the Network Assistant installer.

3. Download the Network Assistant installer, and run it.

   You can run it directly from the Web if your browser offers this choice.

4. When you run the installer, follow the displayed instructions.

5. In the final panel, click Finish to complete the Network Assistant installation.

6. See the Network Assistant online help for more information.

Command Line Interface

You can manage the switch from the command-line interface (CLI) by connecting your personal computer directly to the switch console port or through the network by using Telnet.

Follow these steps to access the CLI through the console port.

1. Connect the supplied RJ45-to-DB-9 adapter cable to the standard 9-pin serial port on the personal computer.
2. Connect the other end of the cable to the console port on the switch.

WARNING

The console port is intended for temporary local programming purposes only and not intended for permanent connection. If you connect or disconnect the console cable with power applied to this module or the programming device on the other end of the cable, an electrical arc can occur. This could cause an explosion in hazardous location installations. Be sure that power is removed or the area is nonhazardous before proceeding.

3. Start a terminal-emulation program on the personal computer.
4. Configure the personal computer terminal emulation software for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.

Switch Software Features

Introduction

The Stratix 8000 and Stratix 8300 switches contain common Ethernet software features, unless otherwise specified.

Topic	Page
Port Numbering	27
Global Macro	29
Smartports	29
VLANs	31
IGMP Snooping With Querier	34
Spanning Tree Protocol	35
Storm Control	36
Port Security	38
EtherChannels	40
DHCP Persistence	41
Precision Time Protocol (PTP)	42
Resilient Ethernet Protocol (REP)	42
SNMP	46
Port Mirroring	49
Layer 3 Routing (Stratix 8300 Switch Only)	50
Alarms	52
Cryptographic IOS Software	52
Advanced Software Features	53

Port Numbering

The port ID consists of port type (Gigabit Ethernet for Gigabit ports and Fast Ethernet for 10/100 Mbps ports), unit number (1, 2, or 3) and port number (1-2 for Gigabits, 1-4 for the 6 port base and 1-8 for all others). Gigabit Ethernet is abbreviated as Gi and Fast Ethernet as Fa.

The following table shows, as an example, port numbering for the 26-port Stratix 8000 switch configuration containing the following:

- One 10-port base switch
- One copper expansion module
- One fiber expansion module

Example Port Numbering for 26 Port Switch[1]

Cat. No.	Unit	Number of Ports	Port Numbering on Switch Labels	Port Numbering in config.txt Text File
1783-MS10T	10-port base switch	10 (2 Gigabit ports and eight 10/100 Mbps ports)	Gigabit ports: 1 2 10/100 Mbps ports: 1 2 3 4 5 6 7 8	Gigabit ports: Gi1/1 Gi1/2 10/100 Mbps ports: Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8
1783-MX08T	Copper expansion module	Eight 10/100 Mbps ports	1 2 3 4 5 6 7 8	Fa2/1 Fa2/2 Fa2/3 Fa2/4 Fa2/5 Fa2/6 Fa2/7 Fa2/8
1783-MX08F	Fiber expansion module	Eight 10/100 Mbps ports	1 2 3 4 5 6 7 8	Fa3/1 Fa3/2 Fa3/3 Fa3/4 Fa3/5 Fa3/6 Fa3/7 Fa3/8

[1] See Appendix B for port numbering for all Stratix 8000 switches.

Global Macro

Once you complete Express Setup (refer to Initialize the Switch with Express Setup on page 17), a global macro (macro name: ab-global) will execute. This macro configures the switch for typical industrial automation applications using the EtherNet/IP protocol. This macro sets many parameters, including these major settings:

- Enable IGMP snooping and Querier
- Enable CIP
- Configure QoS settings and classify CIP, PTP and other traffic
- Enables alarms, SYSLOG, SNMP Notifications
- Enable Rapid Spanning Tree (RSTP), BPDU Guard, BPDU Filter and loop guard

If you do not run Express Setup to initialize the switch, the global macro will not run. The global macro can be run using the CLI.

Smartports

The Smartports port roles are recommended configurations for the switch ports. These configurations (referred to as port roles) optimize the switch connections and ensure security, transmission quality, and reliability for traffic from the switch ports. The port roles also help prevent port misconfigurations.

TIP Use Smartports port roles immediately after the switch initial setup. The switch ports are then correctly configured before they are connected to devices.

Optimize Ports through Smartports Port Roles

The port roles (shown in the following table) are based on the type of devices to be connected to the switch ports. For example, the Desktop for Automation port role is specifically for switch ports to be connected to desktop and laptop computers.

By default, the switch ports are set with the No (None) port role.

Port Role Definitions

Port Role	Description
Automation Device	Apply this role to ports to be connected to Ethernet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O. • Port is set to Access mode. • Port security allows only one MAC ID. • Optimize queue management for CIP traffic.
Automation Device with QoS	Apply this role to ports to a single device that is generating 802.1Q tagged frames (not typically used). • Port is set to Trunk mode (allows 802.1Q Tagged Frames). • Portfast enabled. • Port security allows only one MAC ID.
Desktop for Automation	Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts. • Port is set to Access mode. • Portfast enabled. • Port security allows only one MAC ID. Do not apply to ports to be connected to switches, routers, or access points.
Switch for Automation	Apply this role to ports to be connected to other switches. Port is set to Trunk mode.
Router for Automation	Apply this role to routers or ports to be connected to Layer 3 switches with routing services enabled.
Phone for Automation	Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer would have network access through the port. • Port is set to Trunk mode. • Port security allows three MAC IDs to this port. This role prioritizes voice traffic over general data traffic to ensure clear voice reception on the IP phones.
Wireless for Automation	Apply this role to ports to be connected to wireless access points. The access point can provide network access to up to 30 mobile (wireless) users.
Port Mirroring	Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 49.
None	Apply this role to ports if you do not want a specialized Smartports role on the port. This role can be used on connections to any device, including devices in the roles described above. You can also use this role to connect through a 1783-ETAP module to the Device Level Ring (DLR).

Avoid Smartports Mismatches

A Smartports mismatch occurs when an attached device does not match the Smartports role applied to the switch port. Mismatches can have adverse effects on devices and your network.

Mismatches can result in the following conditions:

- Affect the behavior of the attached device
- Lower network performance (reduce the level of quality of service [QoS]) on CIP, voice, wireless, switch, and router traffic
- Reduce restrictions on guest access to the network
- Reduce protection from denial of service (DoS) attacks on the network
- Disable or shut down the port

We recommend that you always verify which Smartports role is applied to a port before attaching a device to the port or reconnecting devices that have been moved.

VLANs

A virtual local-area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources. For example, VLANs can be based on the departments in your company or by sets of users who communicate mostly with each other.

The switch ships with a default VLAN to which each switch port initially belongs. The switch supports a maximum of 255 VLANs, including the default VLAN.

Every VLAN is identified by its name and ID number. The default VLAN is named default. The ID can be from 1...1001 and 1005...4094, where 1 is the default ID.

You can assign switch ports to either the default VLAN or to VLANs that you have created. The default VLAN alone might be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

The default VLAN is also the management VLAN. After the initial setup, you can create VLANs and designate any VLAN on the switch as the management VLAN. The management VLAN ensures administrative access to the switch. You must assign one of the switch ports to the management VLAN; otherwise, you will not have administrative access to the switch. Initially all ports are assigned to the management VLAN.

You can assign all ports, regardless of their Smartports role, to the default VLAN (default).

Isolate Traffic and Users

By using VLANs, you can isolate different types of traffic (such as voice and data) to preserve the quality of the transmission and to minimize excess traffic among the logical segments. You can also use VLANs to isolate different types of users. For example, you can restrict specific data broadcasts to specific logical workgroups for security purposes, such as keeping information about employee salaries only on devices in a VLAN created for payroll-related communication.

An added benefit to using VLANs is to reduce the amount of administrative effort required to constantly examine requests to network resources.

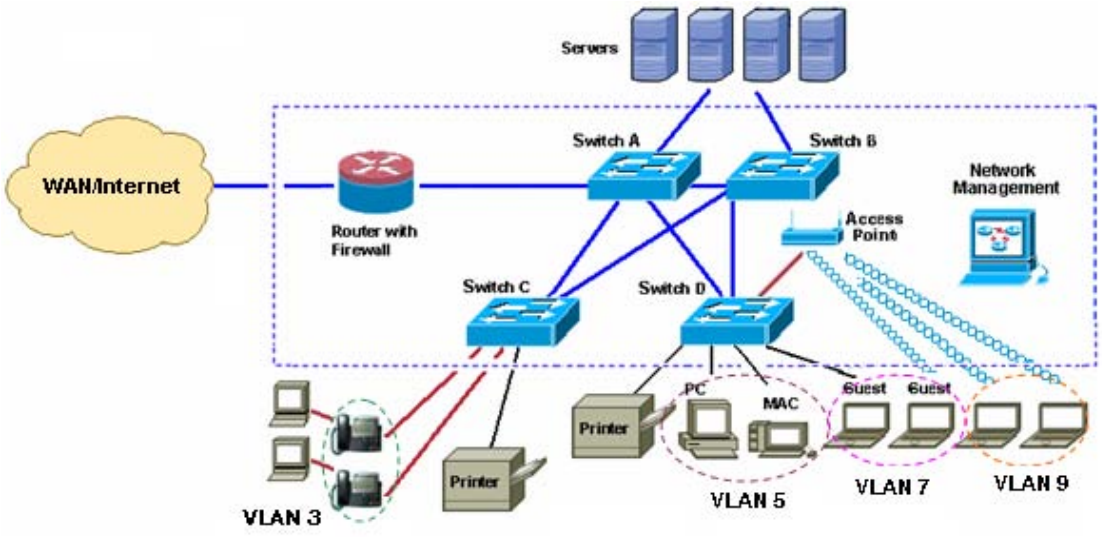
VLANs isolate parts of your network. Therefore, devices that are attached to the switch ports in the same VLAN (network users in the same VLAN) can communicate only with each other and can share the same data.

Devices attached to switch ports in different VLANs cannot communicate with each other through the switch. Inter-VLAN communication requires a router or Layer 3 switch. The router or Layer 3 switch must be configured to allow routing across VLANs (inter-VLAN routing), and additional security policies must be set.

If your network is also using a DHCP server, ensure that the server is accessible to the devices in all the VLANs.

The following figure is an example network that uses VLANs based on different network traffic and network users. Organizing a network around these factors helps to define the size and membership of the VLANs in the network.

VLANs in a Stratix 8000 Switch Network



Isolate Different Traffic Types

Isolating data traffic from delay-sensitive traffic, such as voice traffic, ensures the quality of the voice transmission. In the figure on page 33, VLANs in a Stratix 8000 Switch Network, switch ports connected to the IP phones belong to VLAN 3, a VLAN that is configured to provide Voice over IP (VoIP) services on these connections, meaning priority is given to voice traffic over regular IP data traffic. Voice traffic from the phone and IP-phone service requests to an IP PBX server have priority over traffic from the desktop devices attached to the IP phones.

To further isolate data traffic from voice traffic, the data traffic from the attached desktop devices can be assigned to a separate VLAN.

Group Users

The network shown in the figure on page 33, VLANs in a Stratix 8000 Switch Network provides access to three types of network users: wired employees, wireless (or mobile) employees, and wired and wireless company visitors. Each user type requires different access levels to the company network.

VLANs and security policies on a router or Layer 3 switch can enforce privileges and restrictions to different user types. In the figure on page 33, VLANs in a Stratix 8000 Switch Network:

- VLAN 5 offers employee-level access to the company resources. This kind of network access requires a direct connection to the specific switch ports.
- VLAN 7 offers Internet-only access to company visitors. Visitors with wired or wireless connections to switch ports are assigned to this VLAN, which automatically restricts guest access to only the Internet.
- VLAN 9, which has one or more switch ports connected to the wireless access point, enforces security policies to identify the wireless user (for example, as employee or a guest) and to determine what the user can do on the network (for example, access only the Internet or access other network resources).

IGMP Snooping With Querier

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send join requests and are added to the forwarding table entry. The switch creates one entry per VLAN in the IGMP snooping IP multicast forwarding table for each group from which it receives an IGMP join request.

The switch supports IP multicast group-based bridging, rather than MAC-addressed based groups. With multicast MAC address-based groups, if an IP address being configured translates (aliases) to a previously configured MAC address or to any reserved multicast MAC addresses (in the range 224.0.0.xxx), the command fails. Because the switch uses IP multicast groups, there are no address aliasing issues.

The default number of multicast groups allowed in the switches is as follows:

- Stratix 8000 switch: 256
- Stratix 8300 switch: 1024

You can modify the number of multicast groups supported by using the command line interface.

The IP multicast groups learned through IGMP snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Multicast IP addresses used by the EtherNet/IP network for I/O traffic are learned by the switch.

IGMP implementation in the switch is IGMP V2. This version is backward-compatible with switches using IGMP V1. The switch has a built in querier function, and the global macro enables on IGMP Snooping and the querier.

Spanning Tree Protocol

Spanning Tree Protocol (STP) is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Multiple active paths among end stations cause loops in the network. If a loop exists in the network, end stations might receive duplicate messages. Switches might also learn end-station MAC addresses on multiple Layer 2 interfaces. These conditions result in an unstable network. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

The STP uses a spanning-tree algorithm to select one switch of a redundantly connected network as the root of the spanning tree. The algorithm calculates the best loop-free path through a switched Layer 2 network by assigning a role to each port based on the role of the port in the active topology:

- Root—A forwarding port elected for the spanning-tree topology
- Designated—A forwarding port elected for every switched LAN segment
- Alternate—A blocked port providing an alternate path to the root bridge in the spanning tree
- Backup—A blocked port in a loopback configuration

The switch that has all of its ports as the designated role or as the backup role is the root switch. The switch that has at least one of its ports in the designated role is called the designated switch.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Switches send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The switches do not forward these frames but use them to construct a loop-free path. BPDUs contain information about the sending switch and its ports, including switch and MAC addresses, switch priority, port priority, and path cost. Spanning tree uses this information to elect the root switch and root port for the switched network and the root port and designated port for each switched segment.

Rapid Spanning Tree Protocol

Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1D-2004) uses point-to-point wiring and provides rapid convergence of the spanning tree. RSTP is enabled by default.

TIP If you are connecting the switch to a Cisco network switch, the typical default is PVST+, not RSTP. To provide compatibility, one or the other switch will need to be modified.

Storm Control

Storm control prevents traffic on a LAN from being disrupted by a broadcast, multicast, or unicast storm on one of the physical interfaces. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the protocol-stack implementation, mistakes in network configurations, or users issuing a denial-of-service attack can cause a storm.

Storm control (or traffic suppression) monitors packets passing from an interface to the switching bus and determines if the packet is unicast, multicast, or broadcast. The switch counts the number of packets of a specified type received within the 1-second time interval and compares the measurement with a predefined suppression-level threshold.

Storm control uses one of these methods to measure traffic activity:

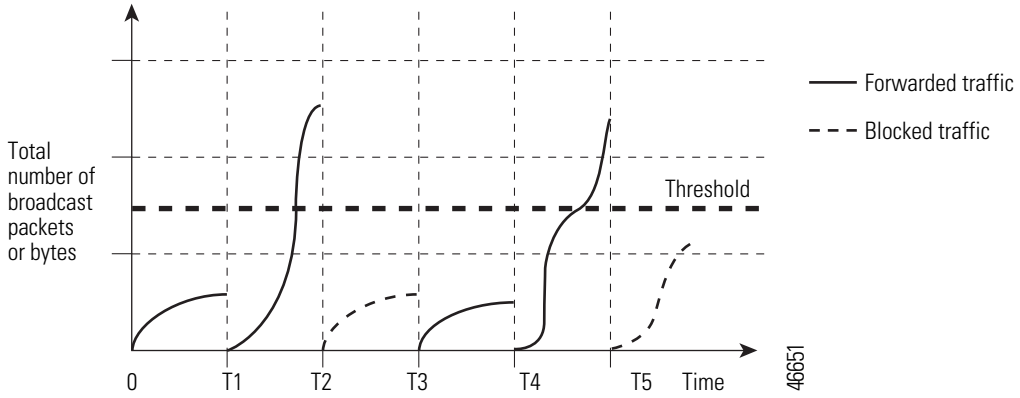
- Bandwidth as a percentage of the total available bandwidth of the port that can be used by the broadcast, multicast, or unicast traffic.
- Traffic rate in packets per second at which broadcast, multicast, or unicast packets are received.
- Traffic rate in bits per second at which broadcast, multicast, or unicast packets are received.

With each method, the port blocks traffic when the rising threshold is reached. The port remains blocked until the traffic rate drops below the falling threshold and then resumes normal forwarding. In general, the higher the level, the less effective the protection against broadcast storms.

IMPORTANT When the storm control threshold for multicast traffic is reached, all multicast traffic except network management traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

The graph shows broadcast traffic patterns on an interface over a given period of time. The example can also be applied to multicast and unicast traffic. In this example, the broadcast traffic being forwarded exceeded the configured threshold between time intervals T1 and T2 and between T4 and T5. When the amount of specified traffic exceeds the threshold, all traffic of that kind is dropped for the next time period. Therefore, broadcast traffic is blocked during the intervals following T2 and T5. At the next time interval (for example, T3), if broadcast traffic does not exceed the threshold, it is again forwarded.

Storm Control Example



The combination of the storm-control suppression level and the 1-second time interval controls the way the storm control algorithm works. A higher threshold allows more packets to pass through. A threshold value of 100% means that no limit is placed on the traffic. A value of 0.0 means that all broadcast, multicast, or unicast traffic on that port is blocked.

IMPORTANT Because packets do not arrive at uniform intervals, the 1-second time interval during which traffic activity is measured can affect the behavior of storm control.

Default Storm Control Configuration

By default, unicast, broadcast, and multicast storm control are disabled. You can set a threshold by using the RSLogix 5000 software.

Port Security

The switch has two methods for limiting the MAC addresses (MAC IDs) that can access a given port:

- dynamic.
- static.

Dynamic Secure MAC Address (MAC ID)

Many Smartport roles have a maximum number of MAC IDs that are allowed to use that port. For example, the Smartport role 'Automation Device' sets up the port for a maximum of one MAC ID. The MAC ID is dynamic, meaning

the switch learns the first source MAC ID to use the port. Attempts by any other MAC ID to access the port will be denied.

If the link becomes inactive, the switch will dynamically relearn the MAC ID to be secured.

The following table shows the Smartport role and the maximum allowable MAC IDs.

Smartport Role	Number of MAC IDs (max)
Automation Device	1
Automation Device With QoS	1
Desktop for Automation	1
Switch for Automation	Not restricted
Router	Not restricted
I/P phone+Desktop	3
Access Point	Not restricted
Port Mirroring	Not restricted
None	Not restricted

Static Secure MAC Address (MAC ID)

The other method of limiting MAC IDs is to statically configure a single MAC ID for a port. This address becomes part of the saved configuration of the switch. This method provides strong security but requires reconfiguration whenever the device connected to the port is replaced, because the new device will have a different MAC ID from the old one.

When you use RSLogix 5000 software to configure the switch Add-on Profile (AOP), you can use the static secure method. This method is not available with the Device Manager Web interface.

Security Violations

It is a security violation when one of these situations occurs:

- The maximum number of secure MAC addresses that have been configured for a port have been added to the address table, and a station whose MAC address is not in the address table attempts to access the interface.

- An address learned or configured on one secure interface is seen on another secure interface in the same VLAN.

When a violation occurs, the port goes into the Restrict mode. In this mode, packets with unknown source addresses are dropped and you are notified that a security violation has occurred. An SNMP trap is sent, a syslog message is logged, and the violation counter increments.

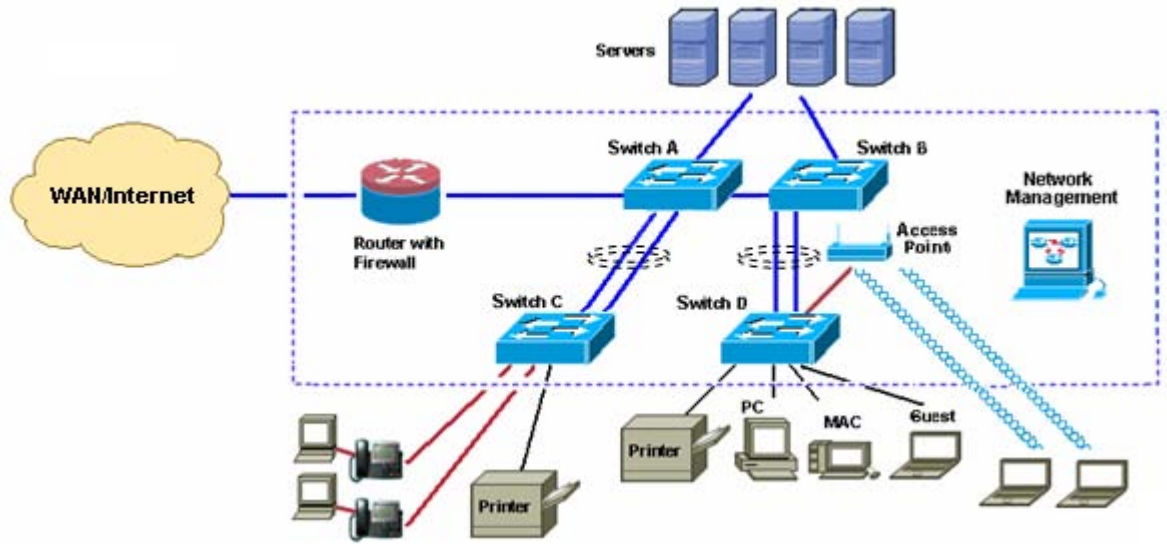
EtherChannels

An EtherChannel (or port group) is a group of two or more Fast Ethernet or Gigabit Ethernet switch ports bundled into a single logical link, creating a higher bandwidth link between two switches. The switch supports up to six EtherChannels. Each EtherChannel can consist of up to eight compatible, configured ethernet ports.

The following figure shows two EtherChannels. Two full-duplex 10/100/1000-Mbps ports on Switches A and C create an EtherChannel with a bandwidth of up to 4 Gbps between both switches. Similarly, two full-duplex 10/100 ports on Switches B and D create an EtherChannel with a bandwidth of up to 400 Mbps between both switches.

If one of the ports in the EtherChannel becomes unavailable, traffic is sent through the remaining ports within the EtherChannel.

EtherChannels between Stratix 8000 Switches



You can configure an EtherChannel in one of these modes: Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), or On. Configure both ends of the EtherChannel in the same mode.

- When you configure one end of an EtherChannel in either PAgP or LACP mode, the system negotiates with the other end of the channel to determine which ports should become active. Incompatible ports are suspended. Instead of a suspended state, the local port is put into an independent state and continues to carry data traffic as would any other single link. The port configuration does not change, but the port does not participate in the EtherChannel.

- When you configure an EtherChannel in the On mode, no negotiations take place. The switch forces all compatible ports to become active in the EtherChannel. The other end of the channel (on the other switch) must also be configured in the On mode; otherwise, packet loss can occur.

If a link within an EtherChannel fails, traffic previously carried over that failed link moves to the remaining links within the EtherChannel. If traps are enabled on the switch, a trap is sent for a failure that identifies the switch, the EtherChannel, and the failed link. Inbound broadcast and multicast packets on one link in an EtherChannel are blocked from returning on any other link of the EtherChannel.

DHCP Persistence

Every device in an IP-based network must have a unique IP address. The Dynamic Host Configuration Protocol (DHCP) automatically assigns IP address information from a pool of available addresses to newly connected devices (DHCP clients) in the network. If a device leaves and then re-joins the network, the device receives the next available IP address, which might or might not be the same address that it had before.

The switch can be set to operate as a DHCP server to provide DHCP persistence. With DHCP persistence, you can assign a specific IP address to each port, ensuring that the device attached to a given port will get the same IP address.

IMPORTANT To make sure DHCP persistence works correctly, follow the application rules. Refer to Configure DHCP Persistence on page 76.

Precision Time Protocol (PTP)

The IEEE 1588 standard defines a protocol, called Precision Time Protocol, or PTP, which enables precise synchronization of clocks in measurement and control systems. The clocks communicate with each other over the EtherNet/IP communication network. The PTP protocol enables heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the grandmaster clock.

Resilient Ethernet Protocol (REP)

The Resilient Ethernet Protocol (REP) provides an alternative to Spanning Tree Protocol (STP) to control network rings and loops, handle link failures, and improve convergence time. REP controls a group of ports connected in a segment, ensures that the segment does not create any bridging loops, and responds to link failures within the segment. REP provides a basis for constructing more complex networks and supports VLAN load balancing.

REP is a segment protocol. One REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (transit) segment ports and two user-configured edge ports. A switch can have no more than two ports that belong to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces. Selecting the Switch for Automation Smartport enables Layer 2 trunking. REP is supported on EtherChannels, but not on an individual port that belongs to an EtherChannel.

You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

These types of REP ports are selectable in the Device Manager Web interface:

- Primary: This port is a primary edge port. This port always participates in VLAN load balancing in the REP segment.
- Edge: This port is a secondary edge port. It also participates in VLAN load balancing in the REP segment.

  Edge ports are termination points of a REP segment. The user must configure two edge ports, including one primary edge port, for each REP segment. Entering edge without primary configures the port as a secondary edge port. Primary and secondary edge ports must be configured even if support of VLAN balancing is not required.

- Transit: This port is a non-edge port in the REP segment.
- No-Neighbor Primary: This port is a primary edge port connected a non-REP switch.
- No-Neighbor: This port is a secondary edge port connected to a non-REP switch.

  The no-neighbor edge ports contain all properties of regular edge ports. These ports allow construction of a REP ring containing a switch that does not support REP protocol.

- None: This port is not part of the REP segment.

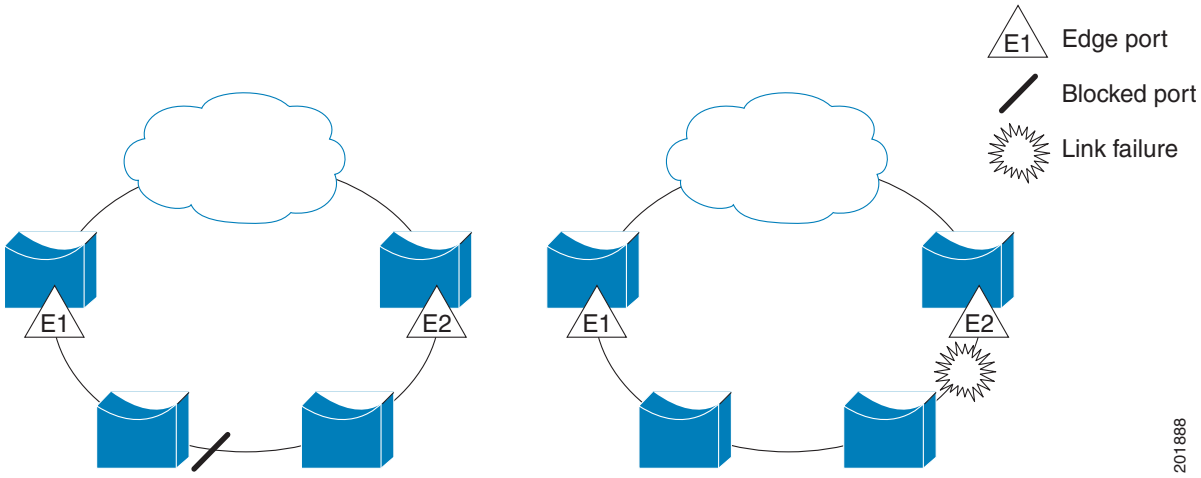
REP and STP can coexist on the same switch, but not on the same port. REP does not interact with STP. For example, if a port is configured as a REP port, STP is disabled on that port. STP bridge protocol data units (BPDUs) are not accepted on or sent from segment ports REP ports. However, adjacent REP and STP rings or domains can share a common link. This common link can be used for passing REP and STP date plane traffic, or for the STP control plane traffic.

The following figure shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a failure in the network, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.

REP Open Segment

The segment shown below is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop and it is safe to connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a failure causes a host to be unable to access its usual gateway, REP unblocks all ports to ensure that connectivity is available through the other gateway.

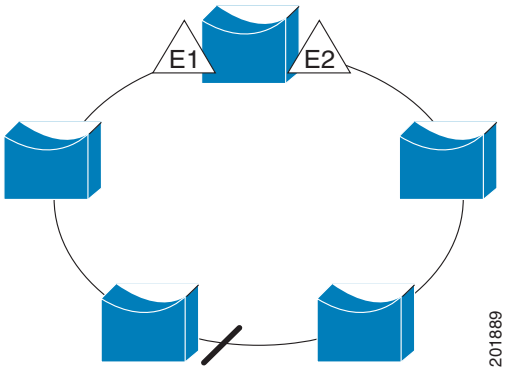
In the following figure, E1 or E2 should be configured as the primary edge port.



REP Ring Segment

The segment shown in the following figure, with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

In the following figure, E1 or E2 should be configured as the primary edge port.



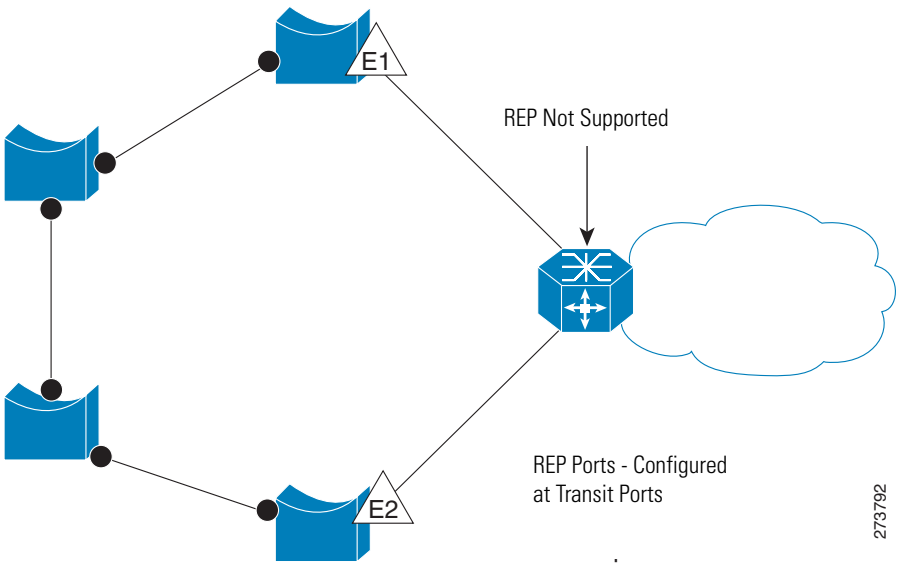
REP segments have these characteristics:

- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.

Access Ring Topologies

In access ring topologies, the neighboring switch might not support REP, as shown in the following figure. In this case, you can configure the non-REP facing ports (E1 and E2) as edge no-neighbor ports. These ports inherit all properties of edge ports, and you can configure them the same as any edge port, including configuring them to send STP or REP topology change notices to the aggregation switch. In this case the STP topology change notice (TCN) that is sent is a multiple spanning-tree (MST) STP message.

In the following figure, E1 or E2 should be configured as the primary no-neighbor port.



REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.

You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared as operational after it performs a three-way handshake with a neighbor in the same segment.

SNMP

The switch supports Simple Network Management Protocol (SNMP) versions 1, 2C, and 3. SNMP allows the switch to be remotely managed through other network management software. This feature is disabled by default.

SNMP is based on three concepts:

- SNMP managers (client software)
- SNMP agents (network devices)
- Management Information Base (MIB)

  Refer to Supported MIBs on page 48 for the MIBs supported on the switch.

The SNMP manager runs SNMP management software. Network devices to be managed, such as bridges, routers, servers, and workstations, have an agent software module. The agent provides access to a local MIB of objects that reflects the resources and activity of the device. The agent also responds to manager commands to retrieve values from the MIB and to set values in the MIB. The agent and the MIB are on the switch. To configure SNMP on the switch, you define the relationship between the manager and the agent.

Both SNMPv1 and v2C use a community-based form of security. SNMP managers can access the agent MIB through passwords referred to as community strings. SNMPv1 and v2C are generally used for network monitoring without network control.

SNMPv3 provides network monitoring and control. It provides secure access to devices by a combination of authenticating and encrypting packets over the network. The security model used by SNMPv3 is an authentication strategy that is set up for a user and the user's group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

Following are some guidelines about SNMPv3 objects.

IMPORTANT SNMPv.3 is available only in the cryptographic version of the switch firmware, available separately.

- Each user belongs to a group.
- A group defines the access policy for a set of users.
- An access policy defines which SNMP objects can be accessed for reading, writing, and creating.
- A group determines the list of notifications that its users can receive.
- A group also defines the security model and the security level for its users.
- An SNMP view is a list of MIBs that a group can access.
- Data can be securely collected from SNMP devices without fear of the data being tampered with or corrupted.
- Confidential information, for example, SNMP Set command packets that change a router configuration, can be encrypted to prevent the contents from being exposed on the network.

Supported MIBs

The following is a list of supported MIBs.

Visit http://www.Cisco.com for the content of each MIB.

- CISCO-ADMISSION-POLICY-MIB
- CISCO-BRIDGE-EXT-MIB
- CISCO-BULK-FILE-MIB
- CISCO-CDP-MIB
- CISCO-CLUSTER-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-DHCP-SNOOPING-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IETF-IP-MIB
- CISCO-IGMP-FILTER-MIB
- CISCO-IMAGE-MIB
- CISCO-L2L3-INTERFACE-CONFIG-MIB
- CISCO-LAG-MIB
- CISCO-MAC-NOTIFICATION-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PAE-MIB
- CISCO-PING-MIB
- CISCO-PORT-QOS-MIB
- CISCO-PORT-SECURITY-MIB
- CISCO-PORT-STORM-CONTROL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-RTTMON-MIB
- CISCO-STACK-MIB
- CISCO-STACKMAKER-MIB
- CISCO-STP-EXTENSIONS-MIB
- CISCO-SYSLOG-MIB
- CISCO-TCP-MIB
- CISCO-UDLDP-MIB
- CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB

- CISCO-VLAN-MEMBERSHIP-MIB
- CISCO-VTP-MIB
- ENTITY-MIB
- ETHERLIKE-MIB
- IEEE8023-LAG-MIB
- IF-MIB
- LLPD-MED-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-IP-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-MIB
- RFC1213-MIB
- RMON-MIB
- RMON2-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMP-VACM-MIB
- SNMPv2-MIB
- TCP-MIB
- UDP-MIB

Port Mirroring

Port mirroring is for advanced users with experience in troubleshooting traffic and protocol issues on networks.

The port mirroring feature copies (or mirrors) traffic on one port to a monitoring port where the packet can be captured by a network protocol analyzer tool. Use port mirroring as a diagnostic tool or debugging feature.

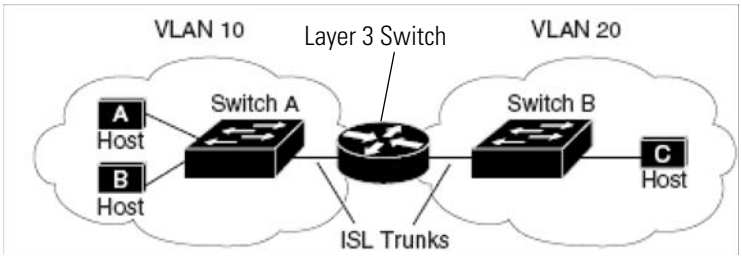
Port mirroring does not affect the switching of network traffic on the monitored port. You must dedicate a monitoring port for port mirroring use. Except for traffic that is being copied for the port mirroring session, the monitoring port does not receive or forward traffic.

Port mirroring can be configured by assigning the Port Mirroring Smartports role on a switch port by using the Device Manager Web interface (see Chapter 3, Manage the Switch via the Device Manager Web Interface).

Layer 3 Routing (Stratix 8300 Switch Only)

The Stratix 83000 Ethernet Managed Switch uses IP address routing to map subnetworks (subnets) to an individual VLAN. In some network environments, VLANs are associated with individual networks or subnetworks. In an IP network, each subnetwork is mapped to an individual VLAN. Configuring VLANs helps control the size of the broadcast domain and keeps local traffic local. However, network devices in different VLANs cannot communicate with one another without a Layer 3 device to route traffic between the VLAN, referred to as inter-VLAN routing. You configure one or more Layer 3 switches to route traffic to the appropriate destination VLAN.

The following figure shows a basic routing topology.



Switch A is in VLAN 10, and Switch B is in VLAN 20. The Layer 3 switch has an interface in each VLAN.

When Host A in VLAN 10 needs to communicate with Host B in VLAN 10, it sends a packet addressed to that host. Switch A forwards the packet directly to Host B, without sending it to the Layer 3 switch.

When Host A sends a packet to Host C in VLAN 20, Switch A forwards the packet to the Layer 3 switch, which receives the traffic on the VLAN 10 interface. The Layer 3 switch checks the routing table, finds the correct outgoing interface, and forwards the packet on the VLAN 20 interface to Switch B. Switch B receives the packet and forwards it to Host C.

Types of Routing

Stratix 8300 switches can route packets by using these methods:

Feature	Description
Static routing	Static routing forwards packets from predetermined ports through a single path into and out of a network. Static routing is secure and uses little bandwidth, but does not automatically respond to changes in the network. Static routing is manually configured by the user for each path in the system.
Dynamic routing	Dynamic routing protocols are used by Layer 3 switches to dynamically calculate the best route for forwarding traffic. There are two types of dynamic routing protocols: • Distance-vector protocols • Link-state protocols Layer 3 switches using distance-vector protocols maintain routing tables with distance values of networked resources, and periodically pass these tables to their neighbors. Distance-vector protocols use one or a series of metrics for calculating the best routes. These protocols are easy to configure and use. Distance-vector protocols supported by the switch are Routing Information Protocol (RIP), which uses a single distance metric (cost) to determine the best path and Border Gateway Protocol (BGP), which adds a path vector mechanism. The switch also supports the Open Shortest Path First (OSPF) link-state protocol and Enhanced IGRP (EIGRP), which adds some link-state routing features to traditional Interior Gateway Routing Protocol (IGRP) to improve efficiency. Routers using link-state protocols maintain a complex database of network topology, based on the exchange of link-state advertisements (LSAs) between routers. LSAs are triggered by an event in the network, which speeds up the convergence time or time required to respond to these changes. Link-state protocols respond quickly to topology changes, but require greater bandwidth and more resources than distance-vector protocols
Unicast routing	Unicast routing is used for all network processes where a private or unique resource is requested.
Multicast routing	In multicast routing, routers create optimal distribution paths for data sent to a multicast destination address spanning tree in real-time. Multicast routing protocols supported are PIM (SM, SM, SDM), DVMRP tunneling.
Redundant routing	Redundant routing localizes the effects of route failures, and reduces control traffic overhead and route reconfiguration time by providing a redundant network path. Redundant routing protocols supported are HSRP (Hot Standby Router Protocol) and CEF (Cisco Express Forwarding).
IPv6 routing	IPv6 network segments, also known as links or subnets, are connected by IPv6 routers, which are devices that pass IPv6 packets from one network segment to another. EIGRP is the supported protocol.
VRF Lite	Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to coexist within the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflicting with each other. The simplest form of VRF implementation is VRF Lite. In this implementation, each router within the network participates in the virtual routing environment in a peer-based fashion.

You can configure static VLAN routing for the Stratix 8300 switch by using the Device Manager Web interface. For more complex routing, use the command-line interface. See the following manuals:

- For more information on these features and how to modify them, see the Cisco IE3000 Switch Software Configuration Manual, available from http://www.Cisco.com.
- For information on using the command-line interface for more complex routing, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Alarms

The switch has two hardware alarm relay contacts on the switch front panel.

- Major alarm relay

  When closed, the major alarm relay indicates a dual-mode power supply or primary temperature alarm.

- Minor alarm relay

  When closed, the minor alarm relay indicates these alarm states:

  – Link fault
  – Port not forwarding
  – Port not operating
  – FCS bit error rate

Cryptographic IOS Software

A separate cryptographic version of the Stratix 8000 and Stratix 8300 IOS is available for ordering from Rockwell Automation. The cryptographic version supports Secure Shell (SSH) Protocol v2 and SNMPv3. This version provides network security by encrypting administrator traffic during Telnet and SNMP sessions. The distribution of the cryptographic IOS is controlled by U.S. export regulations.

Refer to Upgrade the Switch Firmware on page 106 to install the cryptographic IOS software.

Advanced Software Features

More advanced software features are available, some of which are configured by the global macro or Smartports for typical automation applications described in this manual.

For information on how to configure features not available in the Device Manager Web interface or the RSLogix 5000 software AOP, see the following manuals:

- For more information on these features and how to modify them, see the Cisco IE3000 Switch Software Configuration Manual, available from http://www.Cisco.com.
- For information on using the command-line interface for more detailed configuring of these software features, see the Cisco IE3000 Switch Command-Line Interface Manual, available from http://www.Cisco.com.

Notes:

Manage the Switch via the Device Manager Web Interface

Introduction

After you complete Express Setup, you can manage the switch by using the Device Manager Web interface (supplied with the switch).

On all dialog boxes accessible from the Configure menu, when you click Submit, changes are applied to the switch and stored on the CompactFlash card. If you exit the Device Manager Web interface without clicking Submit, your changes are not applied.

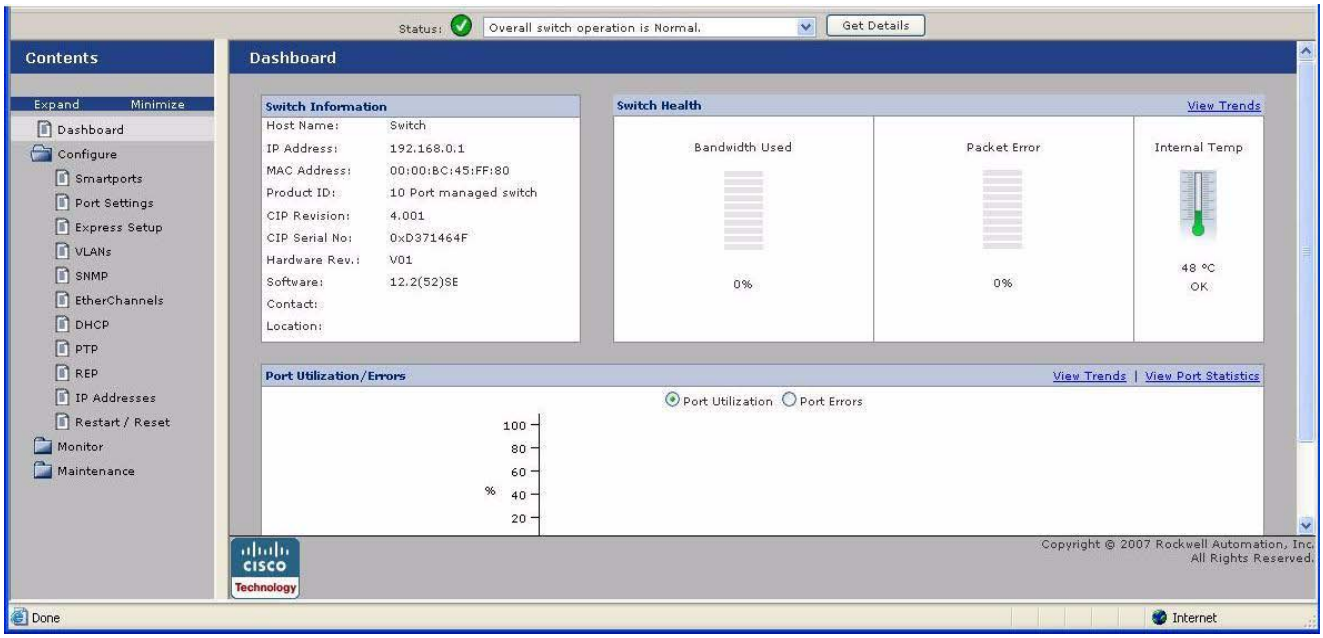
Topic	Page
Access the Device Manager Web Interface	56
Front Panel View and Status Indicators	57
Assign Port Roles	62
Update Switch IP Information	66
Configure VLANs	69
Configure SNMP	72
Configure EtherChannels	75
Configure DHCP Persistence	76
Synchronize the Switch with Other Devices via PTP	83
Configure REP Segments	88
Configure IP Addresses	91
Enable Static Routing (Stratix 8300 Switches Only)	91
Configure Port Mirroring	93
Dashboard Dialog Box	93
Port Status	100
Port Statistics	101
Alert Log	102
CIP Status	104
Upgrade the Switch Firmware	106

Access the Device Manager Web Interface

Follow these steps to use the Device Manager Web interface to configure and monitor the switch.

1. Launch a Web browser on your personal computer or workstation.
2. Enter the switch IP address in the Web browser, and click Enter.

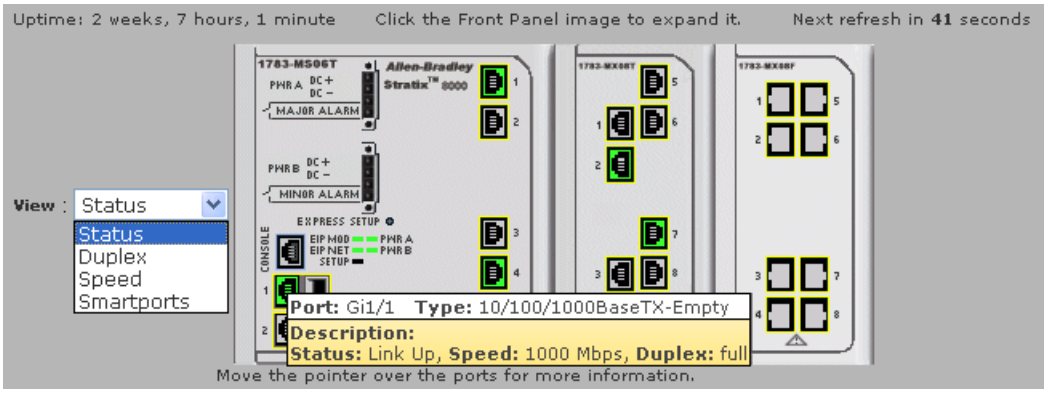
   You see the Device Manager Web interface page.
3. Enter the switch name and password.
4. Use the Device Manager Web interface to perform basic switch configuration and monitoring.



Front Panel View and Status Indicators

The Front Panel view is a graphical display of the front panels of the base switch and attached switch expansion modules, and it is always visible during the Device Manager Web interface session.

Click the Front Panel image to expand or collapse it.


Uptime: 2 weeks, 7 hours, 1 minute
Click the Front Panel image to expand it.
Next refresh in 41 seconds
View : Status
Status
Duplex
Speed
Smartports
Port: Gi1/1 Type: 10/100/1000BaseTX-Empty
Description:
Status: Link Up, Speed: 1000 Mbps, Duplex: full
Move the pointer over the ports for more information.

The switch components on the front panel view are color-coded by status. The colors help you to quickly see if a fault or an error condition exists. The system-level status indicators and port-level status indicators shown on the front panel view match those on the physical switch.

System-level Status Indicators

Status Indicator	Explanation	
EIP Mod	The EIP Mod status indicator shows the status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch is operating properly.
	Blinking green	The switch is not configured (for example, the switch does not have an IP address configured).
	Blinking red	The switch has detected a recoverable system fault. Use the Alert Log to see more details about the problem (see the Alert Log section on page 102).
	Solid Red	The switch has detected a non-recoverable system. Use the Alert Log to see more details about the problem (see the Alert Log section on page 102).
	Blinking green and red	The switch is running its power-on self-test (POST).
EIP Net	The EIP Net status indicator shows the network status of the switch.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	The switch has an established CIP connection to one or more attached devices.
	Blinking green	The switch has an IP address but the switch does not have an established connection to one or more attached devices.
	Blinking red	One or more connections to attached devices have timed out.
	Solid Red	The switch has detected that its IP address is already in use by another device in the network.
	Blinking green and red	The switch is running its power-on self-test (POST).

System-level Status Indicators

Status Indicator	Explanation	
Setup	The Configuration mode in which the switch is operating.	
	Off	The switch is configured as a managed switch or the switch is operating as an unmanaged switch.
	Blinking green	Switch is in the initial Setup mode or is in the Direct Managed mode, or the initial setup is incomplete.
Pwr A and Pwr B	The Pwr status indicators show the DC power status.	
	Off	Power to the switch is off or is not properly connected.
	Solid green	Power is present.
	Solid red	Power to the switch is not present and the power alarm is on.

Status Indicator Mode	Description		
Status	By default, the port status indicators show port status. To display the port duplex mode, the port speed, and the Smartports status from the port status indicators, you must use the **View** list.		
		Off (dark)	No link.
		Solid green	Link is up, but there is no activity on the link.
		Blinking green	Link has activity. During direct managed mode, the port with the blinking green status indicator is the selected management port to which to connect the management station.
		Solid brown	Port is administratively disabled.
		Yellow	Port is error-disabled.
		Blinking green and amber	Link is faulty.
		Blinking amber	Port has a Smartports configuration mismatch.
		Solid amber	Port is faulty, is disabled due to an error condition, or is in an STP-blocked state.
Duplex	In this mode, the port status indicators show the duplex mode (full duplex or half duplex) of the ports. **Note:** The 10/100/1000 ports operate only in full-duplex mode.		
		Off (dark)	No link.
		Solid light blue	Port is in half-duplex mode.
		Solid green	Port is in full-duplex mode.
Speed	In this mode, the port status indicators show the operating speed (10, 100, or 1000 Mb/s) of the ports.		
		Off (dark)	No link.
		Solid light blue	10 Mb/s.
		Solid green	100 Mb/s.
		Blinking green	1000 Mb/s.
Smartports	In this mode, each port image shows the applied port role. For information about Smartports, see Smartports.		

Port-level Status Indicators

Status Indicator Mode	Color	Description
Status		In this mode, the port status indicators show the status of the ports. This is the default mode.
	Off	No link
	Solid green	No activity on link.
	Flashing green	Link activity.
	Solid brown	Port has been disabled.
	Yellow	An error has disabled the port.
	Flashing green and amber	Faulty link.

Port-level Status Indicators

Status Indicator Mode	Color	Description
Status	Flashing amber	Smartports configuration mismatch on port.
	Solid amber	Port is faulty, disabled due to an error, or is in an STP-blocked state.
Duplex		In this mode, the port status indicators show the duplex mode (full-duplex or half duplex) of the ports. The 10/100/1000 ports operate only in full-duplex mode.
	Off	No link.
	Solid light blue	Port is in half-duplex mode.
	Solid green	Port is in full-duplex mode.
Speed		In this mode, the port status indicators show the operating speed (10, 100, or 1000 Mbps) of the ports.
	Off	No link.
	Solid light blue	10 Mbps
	Solid green	100 Mbps
	Flashing green	1000 Mbps
Smartports		In this mode, each port image shows the applied port role. For information about Smartports, see Optimize Ports through Smartports Port Roles on page 29.

You can change the port status indicator behavior by selecting a Port mode from the View list on the front panel view.

Move the pointer over a port to display specific information about the port and its status.

TIP If you move the pointer over a port that is blinking green and amber, the status is one of the following:

- Link is faulty
- Link has collisions

In either state, the port is receiving and sending traffic.

- The speed and duplex mode for a port appear only in the pop-up dialog box when a device is connected to the port.
- For dual-purpose ports, the Type field in the pop-up dialog box displays 10/100/1000BaseTX for the copper uplink port whether or not the port is active. The Type field also displays either the type of SFP module installed or Empty if a module is not installed.
- The Smartport type and VLAN type and name are displayed when Smartport Port mode is selected.

- The Uptime field shows how long the switch has been operating since it was last powered on or was restarted. Status is automatically refreshed every 60 seconds or when you click Refresh. The refresh counter shows the number of seconds that remain before the next refresh cycle starts.

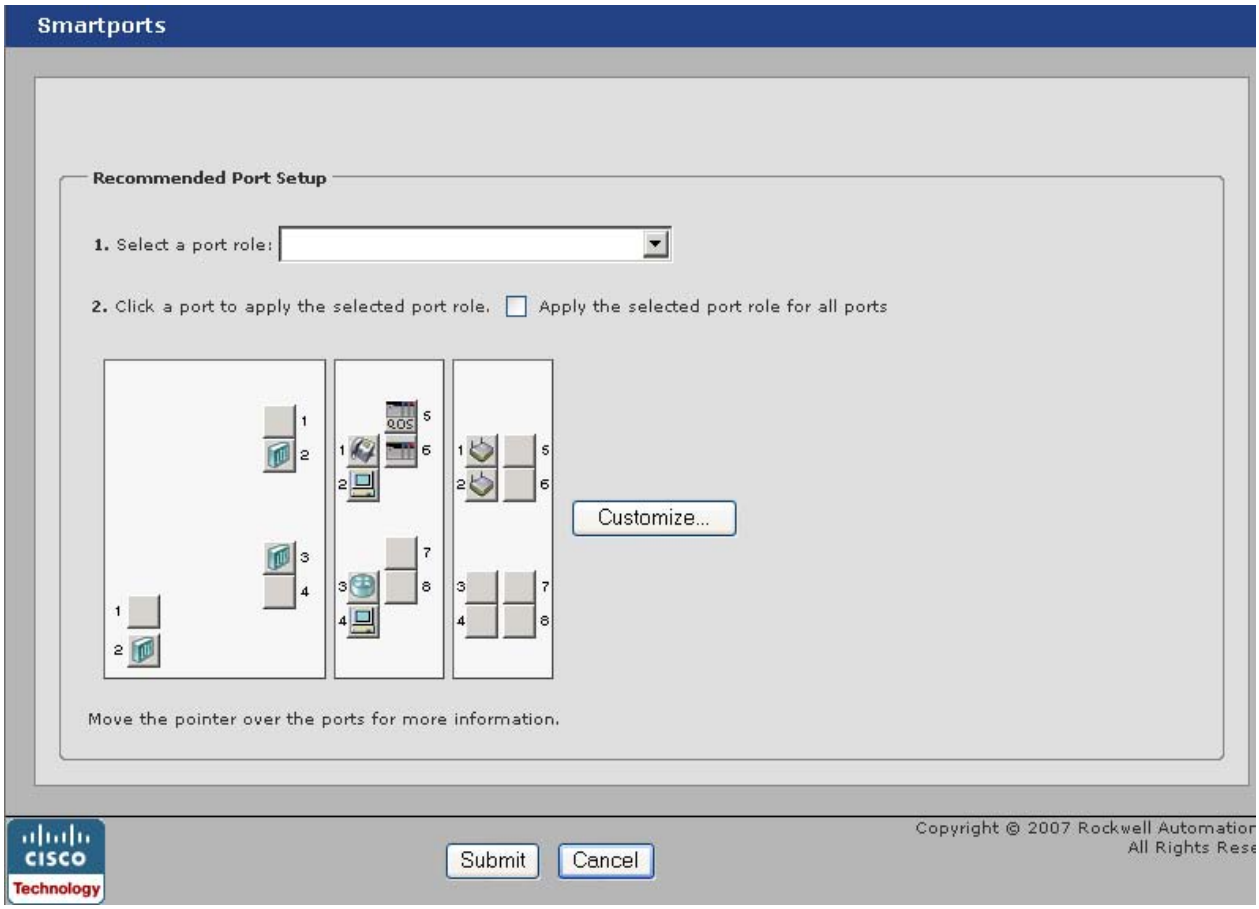
Status Field

The Status field displays the severity and the number of issues (such as hardware and configuration issues) with the switch. If no issues exist, the field shows that the overall switch operation is normal. This field is always visible during the Device Manager Web interface session.The Status field is below the Front Panel view.

Choose an issue in the list, and then click Get Details. This displays a complete troubleshooting report, including the highlighted issue and the recommended actions to resolve the problem.

Assign Port Roles

Use the Smartports dialog box to assign port roles to the switch ports.



Follow these guidelines when using Smartports:

- Before using Smartports, decide which switch port will be connected to which device type.
- Before attaching a device to the port or reconnecting devices that have been moved, verify which Smartports role is applied to a port.

IMPORTANT We recommend that you do not change specific port settings after enabling a Smartports role on a port. Any port setting changes can alter the effectiveness of the Smartports role.

- When the user attempts to apply a port role to a routed port in the Smartports page, this error message displays:

  The selected port is a routed port. A port role cannot be applied to this port.

To assign a Smartport role, follow this procedure.

1. Choose Configure >Smartports from the Device Manager Web interface menu.
2. Select the port role.
3. Click the desired port to which you want to apply the Smartport.
4. To complete the Smartport configuration, refer to Customize Port Role Attributes on page 63.

Customize Port Role Attributes

Each switch port is a member of a VLAN. Devices attached to switch ports that belong to the same VLAN share the same data broadcasts and system resources. Communication between VLANs requires a Layer 3 device (such as a router or a Layer 3 switch).

Depending on your network requirements, it might be sufficient to assign all ports to the default VLAN, which is named default. A small network might only need one VLAN.

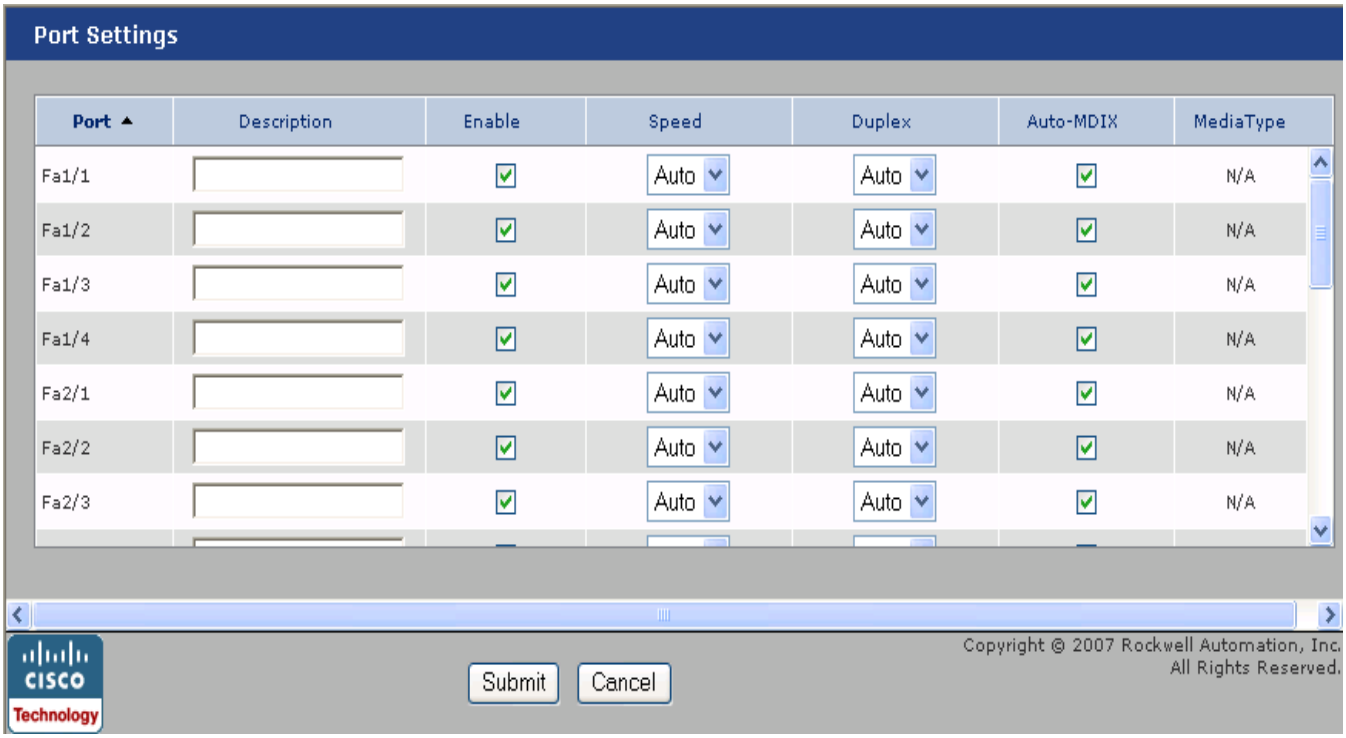
Before changing the virtual local-area network (VLAN) memberships, you should understand what a VLAN is, its purpose, and how to create a VLAN. Refer to VLANs on page 31 for more information about VLANs.

Update Port Settings

The basic port settings determine how data is received and sent between the switch and the attached device. You can change these settings to fit your network needs and to troubleshoot network problems. The settings on a switch port should be compatible with the port settings of the connected device.

Validation blocks the user from configuring port roles for a routed port.

Use the Port Settings dialog box to change basic port settings. To display this dialog box, choose Configure>Port Settings from the Device Manager Web interface menu.



The following table lists the basic settings for the switch ports.

Switch Port Settings

Setting	Description
Port	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch or the switch expansion module number (1, 2, or 3), and the specific port number. For example: • Gi/1 is the gigabit port 1 of the base switch. • Fa1/1 is Fast Ethernet port 1 on the base switch. • Fa2/1 is Fast Ethernet port 1 on the first switch expansion module. • Fa3/1 is Fast Ethernet port 1 on the second switch expansion module.
Description	The description of the switch port. The limit is 18 characters. We recommend that you provide a port description to help identify the port during monitoring and troubleshooting. The description can be the location of the connected device or the name of the person using the connected device.
Enable	The state of the switch port. The default is Enable. Uncheck the selection for the port to administratively (manually) shut down the port. We recommend disabling the port if the port is not in use and is not attached to a device. An example of when to change this setting is during troubleshooting. You can troubleshoot a suspected unauthorized connection by administratively disabling the port.

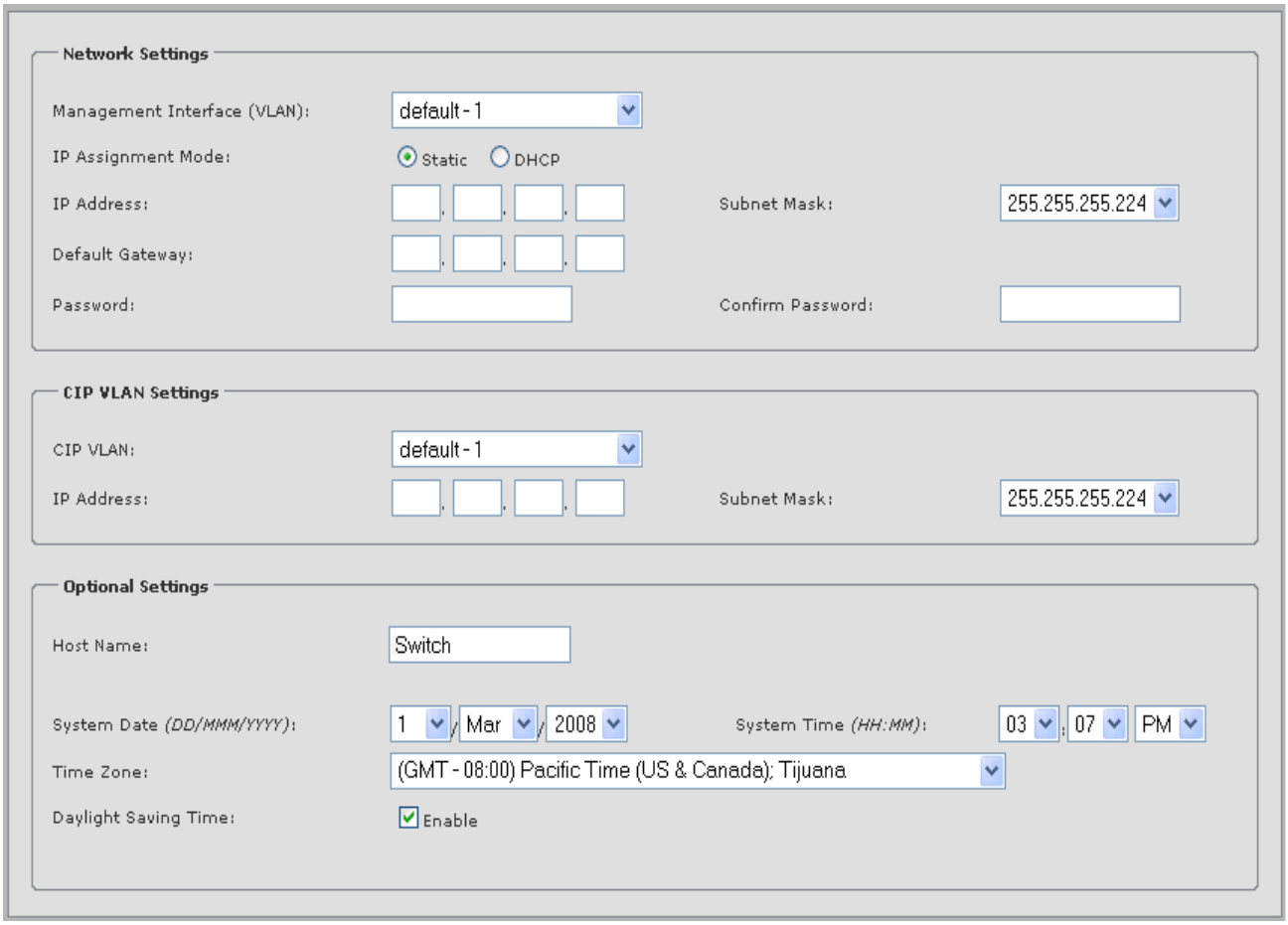
Switch Port Settings

Setting	Description
Speed	The operating speed of the switch port. Choose the speed from the pull-down menu. You can choose Auto (autonegotiation) if the connected device can negotiate the link speed with the switch port. The default is Auto. We recommend that you use the default so that the speed setting on the switch port automatically matches the setting on the connected device. Change the switch port speed if the connected device requires a specific speed. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to see if the switch port and connected device have a speed mismatch. On Gigabit Ethernet ports the speed setting can be set only to auto.
Duplex	The duplex mode of the switch port. Choose the duplex mode from the pull-down menu. Choose one of the following options: • Auto (autonegotiation) if the connected device can negotiate with the switch. • Full (full-duplex) if both devices can send data at the same time. • Half (half duplex) if one or both devices cannot send data at the same time. The default is Auto. On Gigabit Ethernet ports only, you cannot set the port to half duplex if the port speed is set to Auto. We recommend that you use the default so that the duplex setting on the switch port automatically matches the setting on the connected device. Change the duplex mode on the switch port if the connected device requires a specific mode. An example of when to change this setting is during troubleshooting. If you are troubleshooting a connectivity problem, you can change this setting to verify if the switch port and connected device have a duplex mismatch.
Auto-MDIX	Whether the automatic medium-dependent interface crossover (auto-MDIX) feature can automatically detect the required cable connection type (straight-through or crossover) and configure the connection appropriately. The default is Enable. • Uncheck the selection for a port to disable the feature on the port. • To re-enable auto-MDIX, first set the duplex mode and the speed to Auto. This setting is not available on the SFP module ports.
Media Type	The active port type (either the RJ45 port or the SFP module port) of a dual-purpose uplink port. By default, the switch detects whether the RJ45 port or SFP module port of a dual-purpose port is connected and uses the port accordingly. Only one port can be active at a time. If both ports are connected, the SFP module port has priority. You cannot change the priority setting. Choose one of the following selections from the pull-down menu: • SFP if the SFP module port should be active. If you select this option, the speed and duplex displays the current settings, and auto-MDIX displays N/A. • RJ45 if the RJ-45 port should be active. If you select this option, you can set the port speed, duplex, and auto-mdix values. • Auto (autonegotiation) if either port can be active. If you select this option, the speed and duplex is set to auto, and auto-MDIX displays N/A. The default is Auto.

Update Switch IP Information

The network settings enable the switch to operate with its standard default settings and to be managed through the Device Manager Web interface. These settings were set during the initial setup. Change these settings if you want to move the switch to a different management VLAN or to a different network.

Use the Express Setup dialog box to update the switch IP information. To display this dialog box, choose Configure>Express Setup from the Device Manager Web interface menu.



The following tables show switch network settings displayed on the Express Setup dialog box.

Switch Network Settings

Setting	Description
Management Interface (VLAN ID)	The name and ID of the management VLAN through which the switch will be managed. Select an existing VLAN to be the management VLAN. The default ID is 1. The default name for the management VLAN is default. The number can be from 1…001. Make sure that the switch and your network management station are in the same VLAN. Otherwise, you lose management connectivity to the switch. The management VLAN is the broadcast domain through which management traffic is sent between specific users or devices. It provides broadcast control and security for management traffic that should be limited to a specific group of users (such as the administrators of your network). It also ensures secure administrative access to all devices in the network at all times. Refer to VLANs on page 31 for more information about management VLANs and about VLANs in general.
IP Assignment Mode	The IP Assignment mode determines if the switch IP information is manually assigned (static) or is automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you select Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the Device Manager Web interface. If you select DHCP, the DHCP server automatically assigns an IP address, subnet mask, and default gateway to the switch. As long as the switch is not restarted, the switch continues to use the assigned IP information, and you are able to use the same IP address to access the Device Manager Web interface. If you manually assign the switch IP address and your network uses a DHCP server, make sure that the IP address that you give to the switch is not within the range of addresses that the DHCP server will automatically assign to other devices. This prevents IP-address conflicts between the switch and another device.
IP Address	The IP address is a unique identifier for the switch in a network. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0 to 255. This field is enabled only if the IP Assignment mode is Static. Make sure that the IP address that you assign to the switch is not being used by another device in your network. The IP address and the default gateway cannot be the same. You cannot assign the switch with an IP address in the 10.0.0.0 network.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is enabled only if the IP Assignment mode is Static.

Switch Network Settings

Setting	Description
Default Gateway	The IP address for the default gateway. A gateway is a router or a dedicated network device that enables the switch to communicate with devices in other networks or subnetworks. The default gateway IP address should be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. If all of your devices are in the same network and a default gateway is not used, you do not need to enter an IP address in this field. This field is enabled only if the IP Assignment mode is Static. You must specify a default gateway if your network management station and the switch are in different networks or subnetworks. Otherwise, the switch and your network management station cannot communicate.
Password	The password for the switch follows these guidelines: • Can have up to 63 alphanumeric characters • Can start with a number • Is case sensitive • Can have embedded spaces. • Cannot be a single digit • Cannot contain a ? or a tab • Does not allow spaces at the beginning or the end This password is also used as the Control and Information Protocol (CIP) security password. You must provide a password to the switch to secure the access to the Device Manager Web interface.
Confirm Password	Enter the switch password again.

CIP VLAN Settings

Setting	description
CIP VLAN	The VLAN on which CIP will be enabled. The CIP VLAN can be the same as the management VLAN or you can isolate CIP traffic on another VLAN that is already configured on the switch. Change the CIP VLAN settings only if you want CIP traffic to be on a separate VLAN from the management VLAN. Existing settings might have been set during the initial setup (done through the Express Setup process; refer to Initialize the Switch with Express Setup on page 17). The default ID is 1. The default name for the CIP VLAN is default.
IP Address	The IP address is a unique identifier for the switch in a network. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0...255. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.
Subnet Mask List	The subnet mask is the network address that identifies the subnetwork (subnet) to which the switch belongs. Subnets are used to segment the devices in a network into smaller groups. The default is 255.255.255.0. If the CIP VLAN is different from the management VLAN, you must specify a subnet mask for the CIP VLAN.

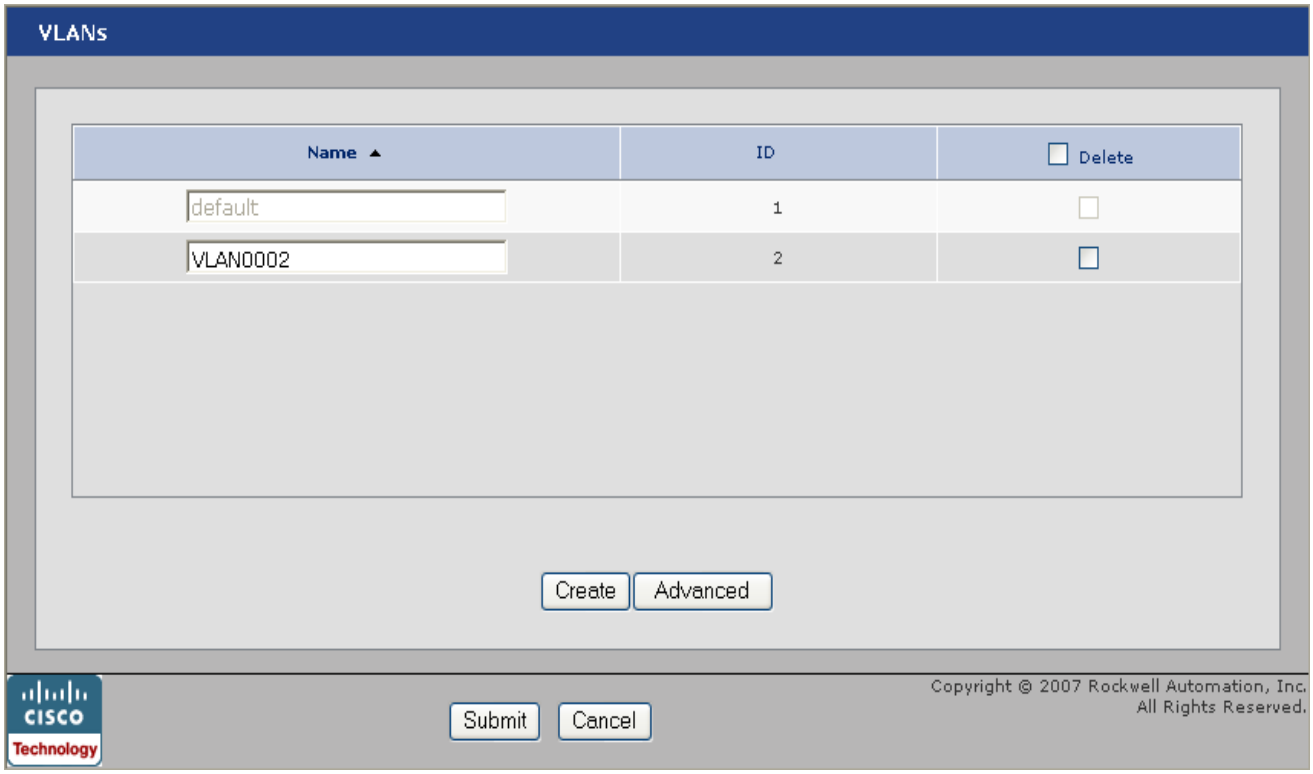
TIP The following settings will reset if power to the switch is lost. To maintain these settings, connect the switch to a Network Time Protocol (NTP) server by using the command-line interface.

Optional Settings

Setting	Description
Host Name	A name for the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ?, a space, or a tab. The default is Switch. We recommend entering either the name, the location, or the IP address of the switch to help identify the switch during monitoring or troubleshooting.
System Date	The date that the switch read from the network management station or that was manually set during the initial setup. If you change the date, the change takes effect immediately after you click Submit.
System Time	The time that the switch read from the network management station or that was manually set during the initial setup. If you change the time, the change takes effect immediately after you click Submit.
Time Zone	This is the time zone that the switch automatically read from the network management station or that was manually set during the initial setup. If you change the time zone, the change takes effect immediately after you click Submit.
Daylight Savings Time	Automatically checked only when the selected time zone is in the U.S., Europe, or Australia. Unchecked for all other time zones.

Configure VLANs

Use the VLANs dialog box to create, modify, and delete VLANs. To display this dialog box, choose Configure>VLANs from the Device Manager Web interface menu.



The default VLAN ID is 1 and the name for the management VLAN is default. The default VLAN alone might be sufficient based on the size and requirements of your network. We recommend that you first determine your VLAN needs before creating VLANs.

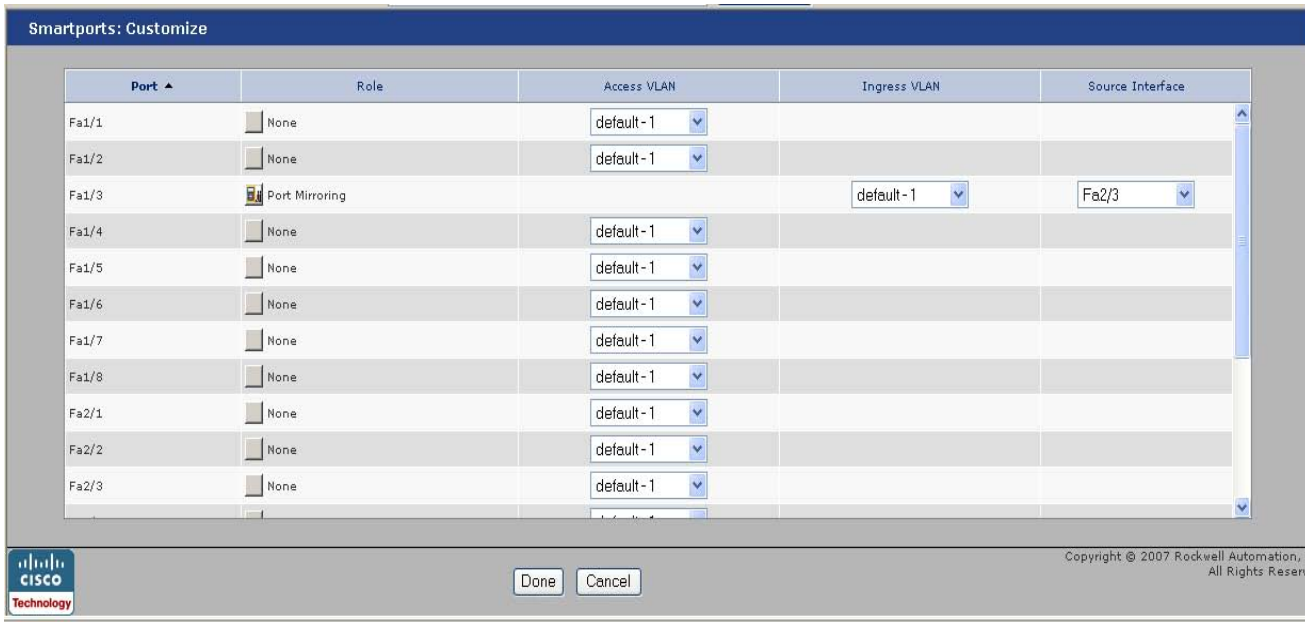
To create a VLAN, you must give the VLAN a name and a unique ID number. You can create up to 255 VLANs.

You can modify the name of a VLAN but not its number. You cannot modify or delete the default VLAN.

After creating VLANs, you can then assign the appropriate ports to those VLANs. Before assigning ports to VLANs, make sure that each port is applied with the appropriate port role.

Assign Ports to VLANs

To display this dialog box, choose Configure>Smartports from the Device Manager Web interface menu, and click Customize on the Smartports dialog box.



Advanced VLAN Configuration

The advanced VLAN options are the Rapid Spanning Tree Protocol (RSTP) and the Internet Group Management Protocol (IGMP) snooping features on the switch ports. These options are enabled by default.

We recommend that you leave these options enabled for the benefits that they provide.

IMPORTANT Disabling RSTP can affect connectivity to the network. Because many EtherNet/IP applications use multicast extensively, disabling IGMP snooping can adversely affect the network performance.

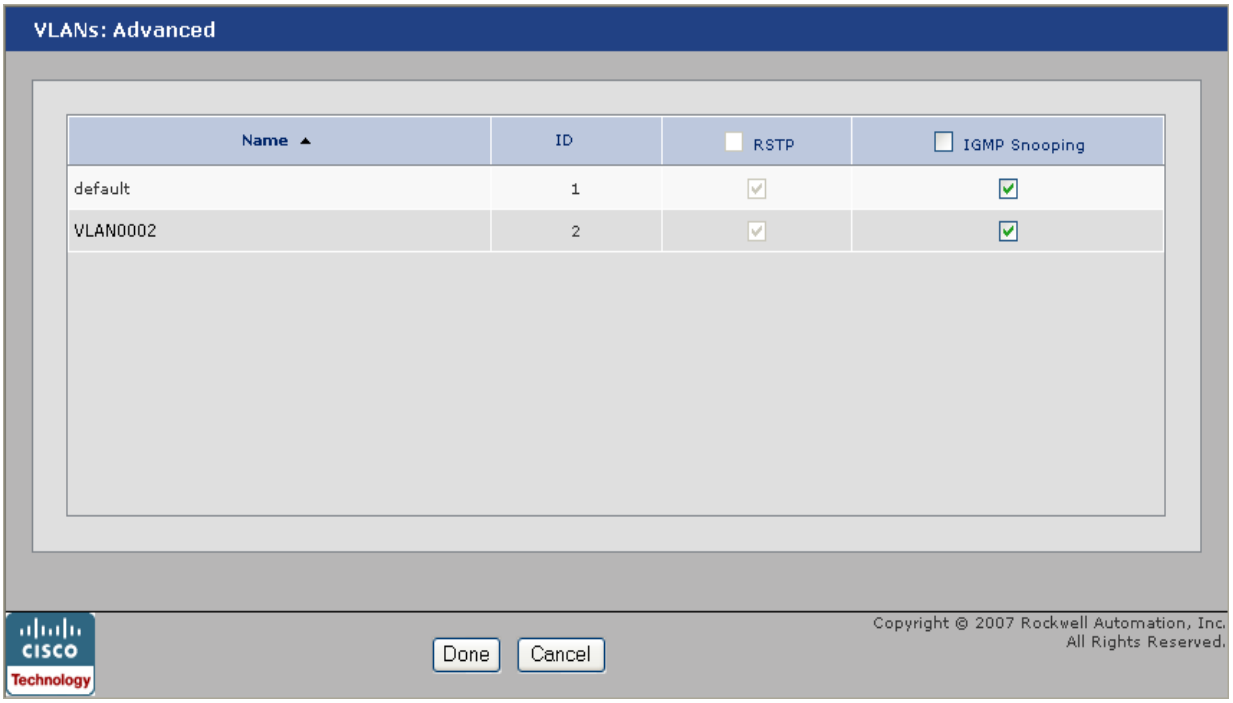
- RSTP prevents network loops by enabling only one active path for traffic to use.

  RSTP also provides a redundant path if the active path becomes unavailable.

- IGMP snooping reduces duplicate and excess traffic on the network by forwarding IP multicast traffic to specific switch ports rather than by flooding all ports.

  With IGMP snooping, only ports that are members of specific IP multicast groups receive multicast messages. The result is a more efficient use of bandwidth.

Use the VLANs Advanced dialog box to change the RSTP and IGMP snooping settings. To display this dialog box, choose Configure>VLANs from the Device Manager Web interface menu, and then click Advanced on the VLANs dialog box.

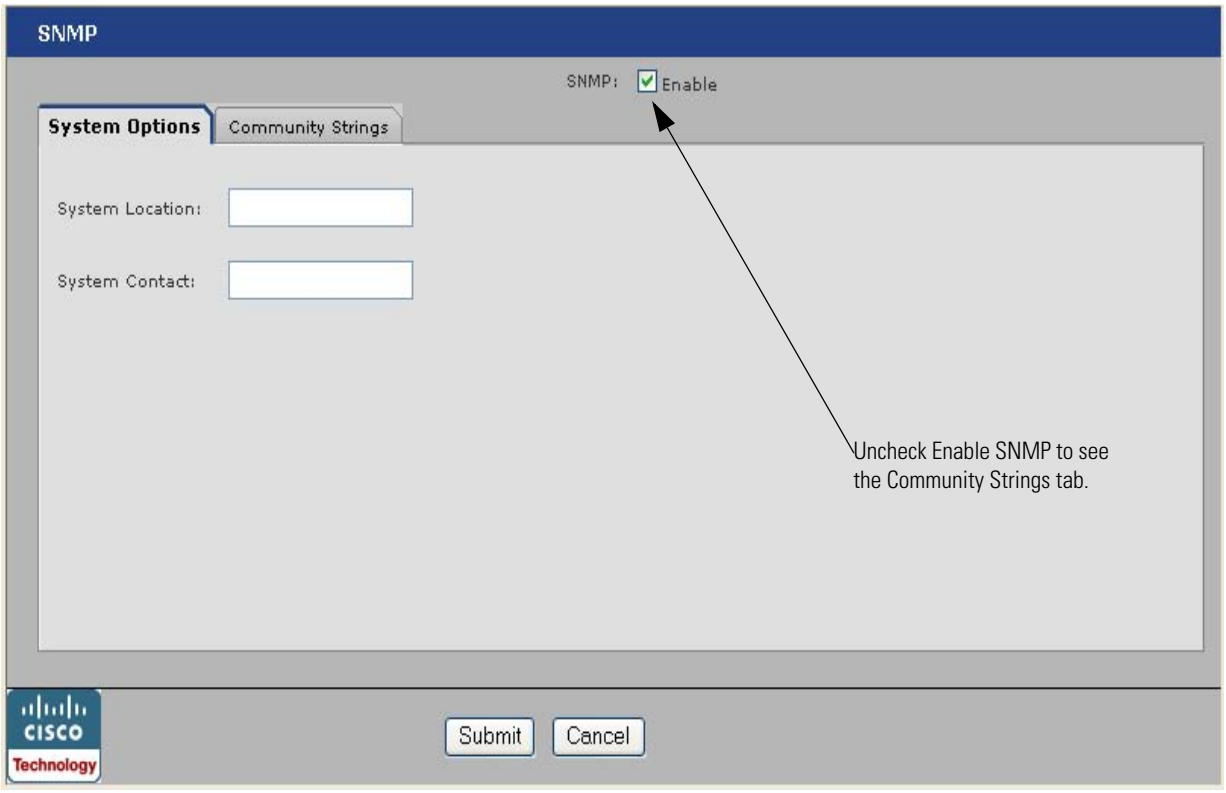


Configure SNMP

Enable SNMP if you plan to have the switch managed through another network management application. By default, SNMP is disabled.

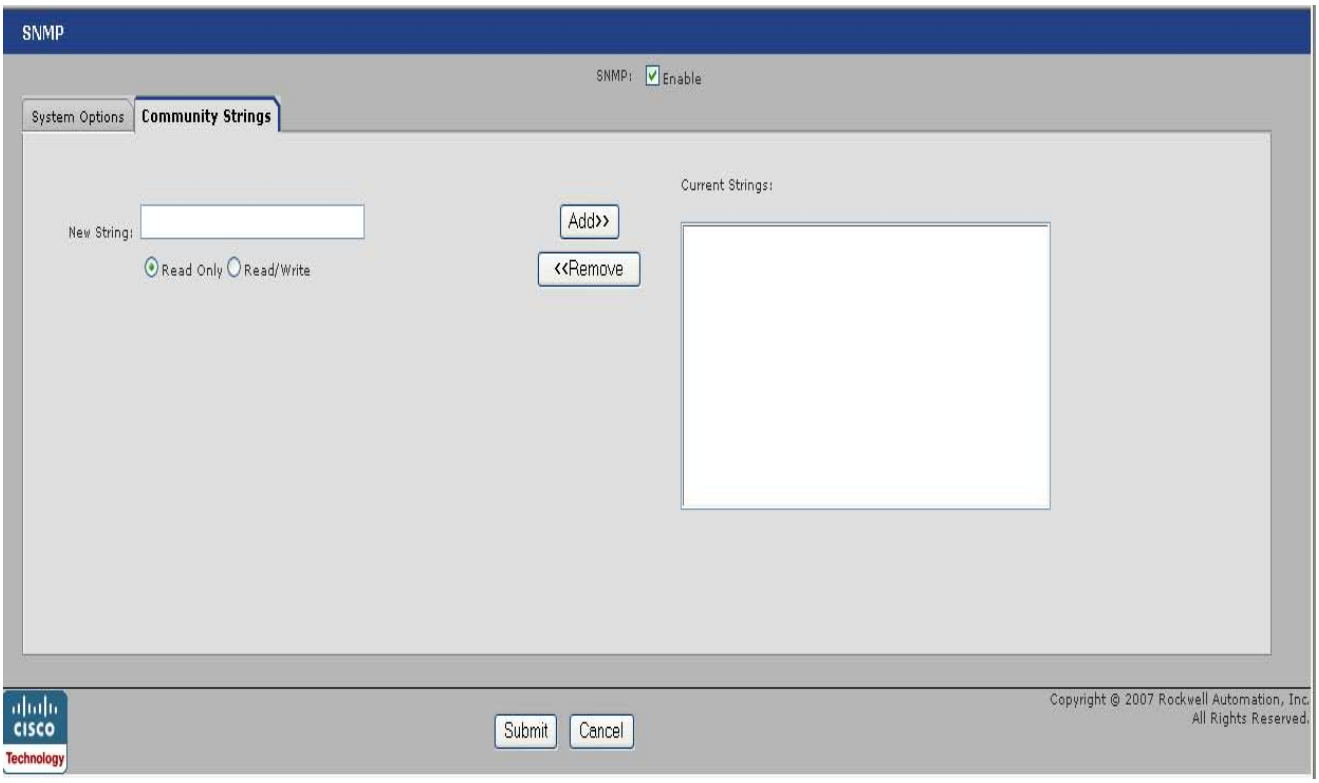
Other general SNMP settings include the name of the switch or the network administrator and the switch location. The system name and the system contact information appear in the Switch Information area on the Dashboard.

Use the SNMP dialog box to update change the SNMP settings. To display this dialog box, choose Configure>SNMP from the Device Manager Web interface menu.



Community strings are passwords to the switch Management Information Base (MIB). You can create community strings that allow a remote manager read-only or read-write access to the switch.

Click the Community Strings tab to display the Community Strings dialog box. Enable SNMP must be unchecked so that the Community Strings tab appears.



- The Read-Only community string enables the switch to validate Get (read-only) requests from a network management station.

  If you set the SNMP read community, users can access MIB objects, but cannot change them.

- The Read-Write community string enables the switch to validate Set (read-write) requests from a network management station.Use SNMP Management Applications

You can use SNMP management applications such as IntraVue or HP OpenView to configure and manage the switch. Refer to SNMP on page 46 for more information.

Configure EtherChannels

You can create up to six EtherChannels, and you can configure each EtherChannel in one of these modes.

- IEEE 802.3ad (LACP) mode (default)

  This allows the switch to create one end of the EtherChannel if the other switch requests it.

- Static mode

  This mode requires you to make sure that both ends of the EtherChannel have the same configuration and then to manually create the EtherChannel.

- Port Aggregation Protocol (PAgP) mode

  This mode allows the switch to automatically form an EtherChannel with the other switch.

Use the EtherChannels dialog box to create, modify, and delete EtherChannels. To display this dialog box, choose Configure>EtherChannels from the Device Manager Web interface menu.

See the Device Manager Web interface online help for additional guidelines and procedures.

All ports in an EtherChannel must have the same characteristics.

- All are either 10/100 ports, or all are 10/100/1000 ports.

  You cannot group a mix of 10/100 and 10/100/1000 ports in an EtherChannel.

- All have the same speed and duplex mode settings.

  A mismatch in speed or duplex disables the EtherChannel.

- All are enabled.

  A disabled port in an EtherChannel is treated as a link failure, and its traffic is transferred to one of the remaining ports in the EtherChannel.

- All are applied with the Smartports Switch for Automation port role and belong to the same VLAN.

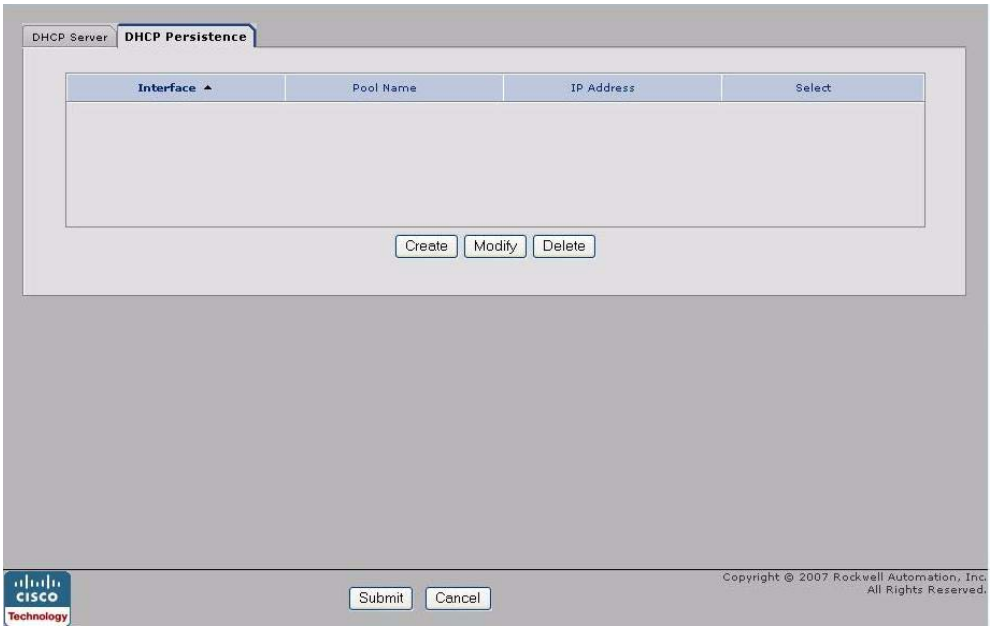
Configure DHCP Persistence

To use DHCP persistence, you must first enable DHCP and set up the IP address pool. Then you must assign a specific IP addresses to each port.

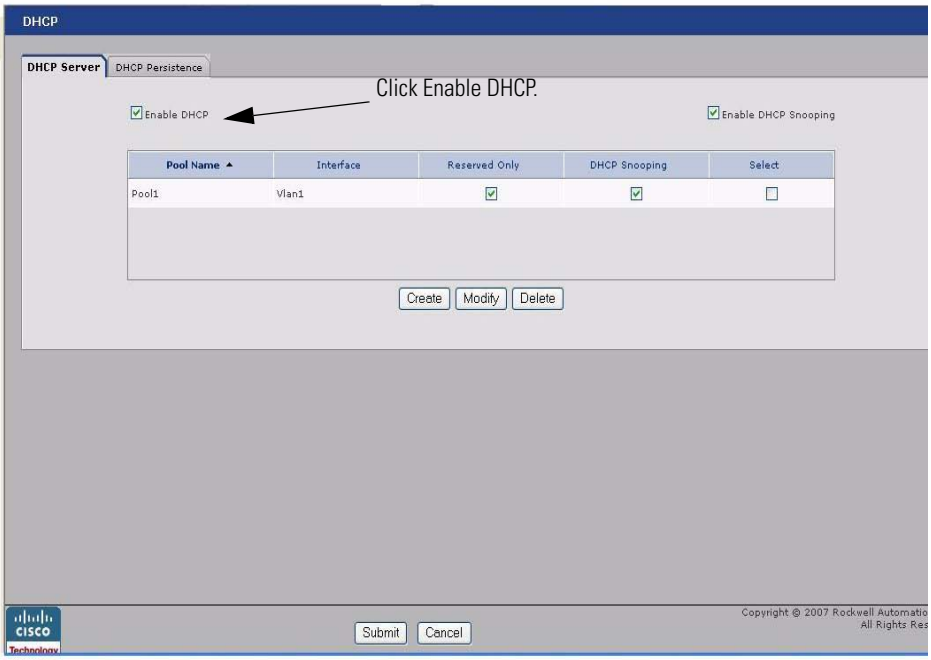
Set up the DHCP Server

To enable or disable the DHCP server mode on the switch, do the following.

1. Choose Configure>DHCP from the Device Manager Web interface.



2. Click Enable DHCP.



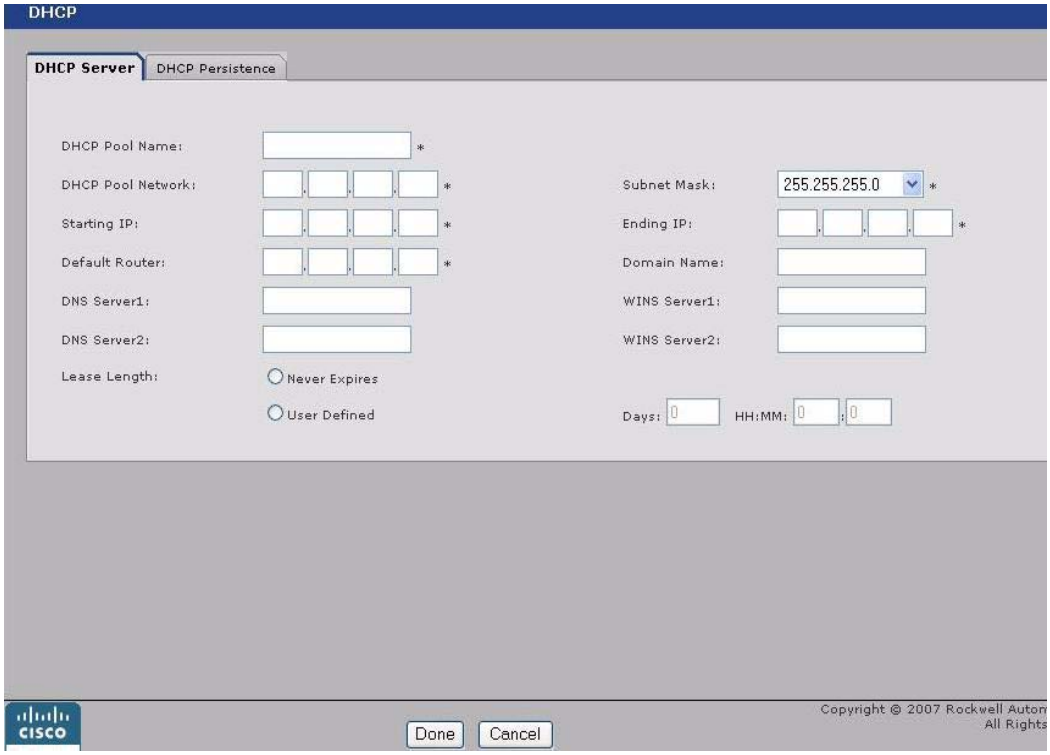
3. Enter DHCP server settings, as appropriate.

Setting	Description
Reserved Only	This option reserves the address pool to only the devices that are specified in the DHCP persistence table. DHCP requests from ports not in the persistence table or from another device (switch) are ignored. By default, this option is disabled (the Reserved Only check box is not selected). Select this option if you do not want unassigned IP addresses in the pool to be assigned to a port that is not in the DHCP persistence table.
Enable DHCP Snooping	DHCP snooping restricts broadcast of DHCP requests beyond the connected switch.This means that devices will receive address assignments only from the connected switch. This option is available only on VLAN interfaces. To enable DHCP Snooping on a specific VLAN check the Enable DHCP Snooping box and the DHCP Snooping box for the specific VLAN desired.
DHCP Snooping	To enable DHCP Snooping on a specific Vlan check the Enable DHCP Snooping box and the DHCP Snooping box for the specific VLAN desired.

Configure a DHCP IP Address Pool

Once DHCP is enabled, you can create the DHCP address pool from the DHCP dialog box.

1. Click Create.



2. Enter DHCP Address Pool settings, as appropriate.

DHCP Address Pool Settings

Setting	Description
DHCP Pool Name	The name of the DHCP IP address pool configured on the switch. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab. This field is required. A DHCP IP address pool is a range (or pool) of available IP addresses that the switch can assign to connected devices.
DHCP Pool Network	The subnetwork IP address of the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. This field is required.
Subnet Mask	The network address that identifies the subnetwork (subnet) of the DHCP IP address pool. Subnets segment the devices in a network into smaller groups. The default is 255.255.255.0. This field is required.
Starting IP Address	The starting IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Be sure that none of the IP addresses that you assign are being used by another device in your network. This field is required.
Ending IP Address	The ending IP address that defines the range of addresses in the DHCP IP address pool. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255. Make sure that none of the IP address you assign are being used by other devices in your network. This field is required.
Default Router	The default router IP address for the DHCP client that will be using this server. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0… 255. This field is required.
Domain Name	The domain name for the DHCP client. The name can have up to 31 alphanumeric characters. The name cannot contain a ? or a tab.
DNS Server1 and 2	The IP addresses of the Domain Name System (DNS) IP servers available to a DHCP client. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255.
WINS Server1 and 2	The IP addresses of the primary and secondary Microsoft NetBIOS name servers (WINS servers) available to a DHCP client. The format is a 32-bit numeric address written as four numbers separated by periods. Each number can be from 0…255.
Lease Length	The duration of the lease for an IP address that is assigned to a DHCP client. Click either: • Never Expires • User Defined If you click User Defined, enter the duration of the lease in the numbers of days, hours, and minutes. This lease length is used for all assignments.

3. Click Done.

Reserve IP Addresses through DHCP Persistence

You can reserve and preassign an IP address from the IP address pool to a specific switch port, so that a device connected to that switch port always receives the same IP address regardless of its MAC address.

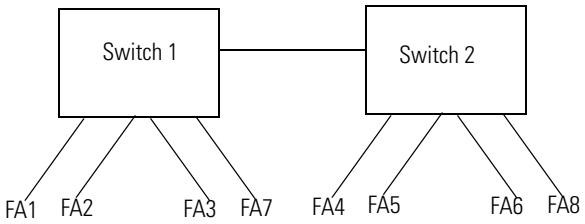
DHCP persistence is useful in networks that are set up in advance, where dependencies on the exact IP addresses of some devices exist. Use DHCP persistence when the attached device has a specific role to play and when other devices know its IP address. If the device is replaced, the replacement device is assigned the same IP address, and the other devices in the network require no reconfiguration.

When the DHCP persistence feature is enabled, the switch acts as a DHCP server for other devices on the same subnet, including devices connected to other switches (including other Stratix 8000 switches). If the switch receives a DHCP request it will respond with any unassigned IP addresses in its pool. To prevent this from happening, check the Reserve Only box on the DHCP dialog box. This ensures that the switch will not respond when a request is received.

When the DHCP persistence feature is enabled on a port and a DHCP request is made from a connected device on that port, the switch assigns the IP address for that port in the DHCP dialog box. It will also broadcast the DHCP request to the remainder of the network. If another DHCP server with available addresses is on the network and receives this request it may try and respond. This may override the initial IP address assigned by the switch depending on how the end device behaves (takes first IP address response or the last). To prevent the IP address from being overridden, enable DHCP snooping on the appropriate VLAN. Doing this blocks the broadcast of this DHCP request so that no other server (including another Stratix 8000 or Stratix 8300 switch with DHCP persistence enabled) will respond.

If you are using DHCP persistence, we recommend that you initially assign static IP addresses to end devices. If an end device fails and is replaced, the DHCP persistence feature assigns an IP address from the DHCP persistence table. The device will function properly with this IP address, but you should reassign a static IP address to the replaced devices.

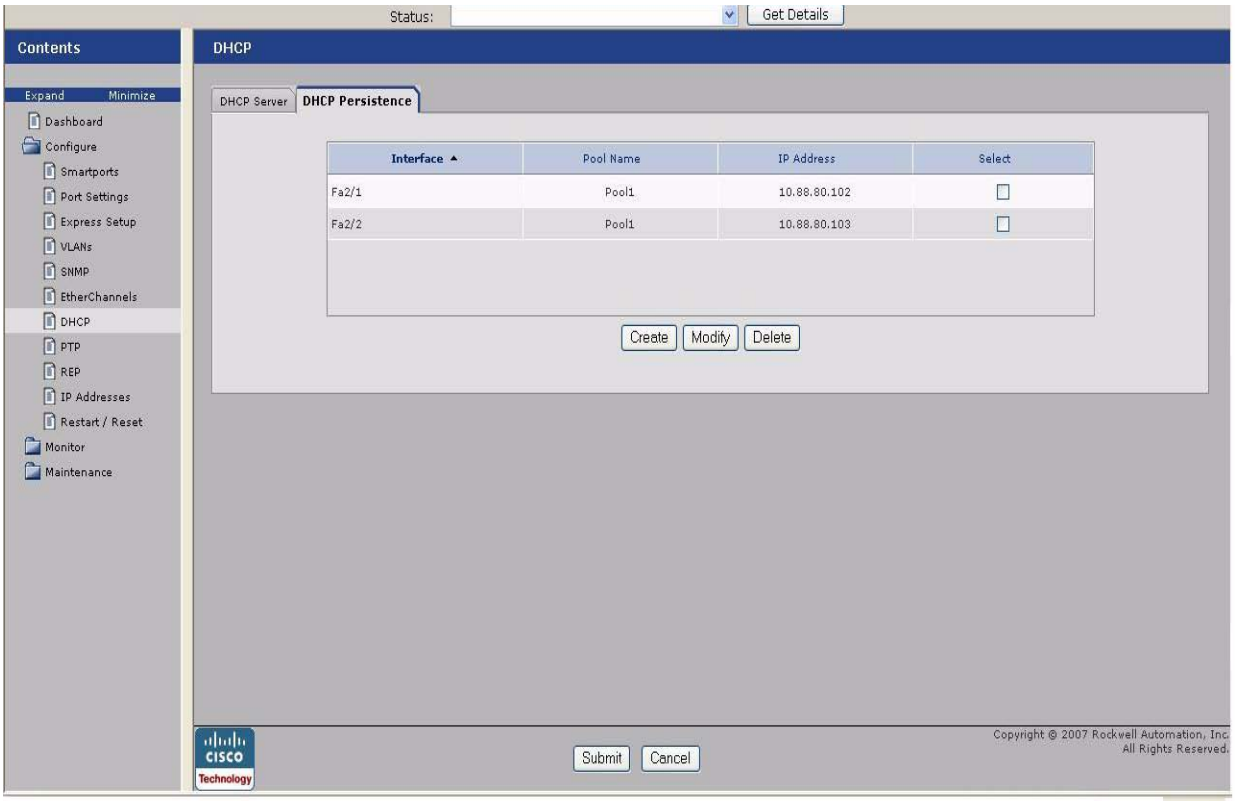
The following figure and chart illustrate DHCP persistence behavior.



If	Then
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is not selected and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 will respond if there is an unassigned address in its pool. This may override the assignment made by switch 1.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in both switches and DHCP snooping is off	A new device connected to switch 1 FA1 receives an IP address from the switch 1 persistence table. A broadcast request is also sent across the network. Switch 2 will not respond to the request. Note that if the device is connected to FA7 of switch 1, it will not receive an IP address from the switch pool, since it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • Reserve Only is selected in switch 1 and DHCP snooping is off, but not switch 2 when DHCP snooping is off	A new device is connected to FA1 receives an IP address from the persistence table. A broadcast request is also sent across the network. Switch 2 will not respond to the request. In addition, a device connected to FA4 receives an IP address from the switch 2 persistence table. A broadcast request is sent out, and switch 1 responds with an unused IP address from its pool.This may override the assigned port.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved only is selected	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 will not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it will not receive an IP address from the switch pool, since it is not defined in the persistence table, and unused addresses in the pool are blocked.
• Switch 1 has ports FA1…FA3 in its persistence table • Switch 2 has ports FA4, FA5, FA6 and FA8 in its persistence table • DHCP Snooping is selected • Reserved only is not selected	A new device connected to switch 1 FA1 receives an IP address from the Switch 1 persistence table. A broadcast request is not sent across the network, therefore Switch 2 will not respond. Note that if a device is connected to FA7 (not defined in the DHCP persistence table) of Switch 1, it will receive an unassigned IP address from the Switch 1 pool.

Use the DHCP Persistence dialog box to assign, modify, or delete a switch port IP address.

1. Click the DHCP Persistence tab.



2. Enter DHCP Persistence settings, as appropriate.

DHCP Persistence Settings

Setting	Description
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch or the switch expansion module number (1, 2, or 3), and the specific port number. For example: Fa1/1 is Fast Ethernet port 1 on the base switch. Fa2/1 is Fast Ethernet port 1 on the first switch expansion module. Fa3/1 is Fast Ethernet port 1 on the second switch expansion module.
Pool Name	The name of the DHCP IP address pool configured on the switch.
IP Address	The IP address assigned to the switch port. The IP address that you assign is reserved for the selected port and is not available for normal DHCP dynamic assignment. The IP address must be an address from the pool specified in the DHCP Pool Name field.

3. Click Done.

Synchronize the Switch with Other Devices via PTP

The IEEE 1588 standard defines a protocol, called Precision Time Protocol, or PTP, which enables precise synchronization of clocks in measurement and control systems. The clocks communicate with each other over the EtherNet/IP communication network. The PTP protocol enables heterogeneous systems that include clocks of various inherent precision, resolution and stability to synchronize. PTP generates a Master-Slave relationship among the clocks in the system. All clocks ultimately derive their time from a clock selected as the grandmaster clock.

By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports on the base switch module. Only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP.

IMPORTANT Do not connect PTP-capable devices to expansion ports. All PTP packets received by a non-PTP-capable port on a switch supporting PTP are discarded.

The switch supports two synchronization clock modes:

- **End-to-End Transparent mode** The switch transparently synchronizes all slave clocks with the master clock connected to the switch. This is the default mode.

  The switch corrects the delay incurred by every packet passing through the switch (referred to as residence time). This mode causes less jitter and error accumulation than boundary mode.

  In End-to-End Transparent mode, all switch ports in the base are enabled.

- **Boundary mode** The switch becomes the parent clock to which the other devices connected to the switch synchronize their internal clocks.

  The switch and connected devices constantly exchange timing messages to correct time skew caused by clock offsets and network delays.

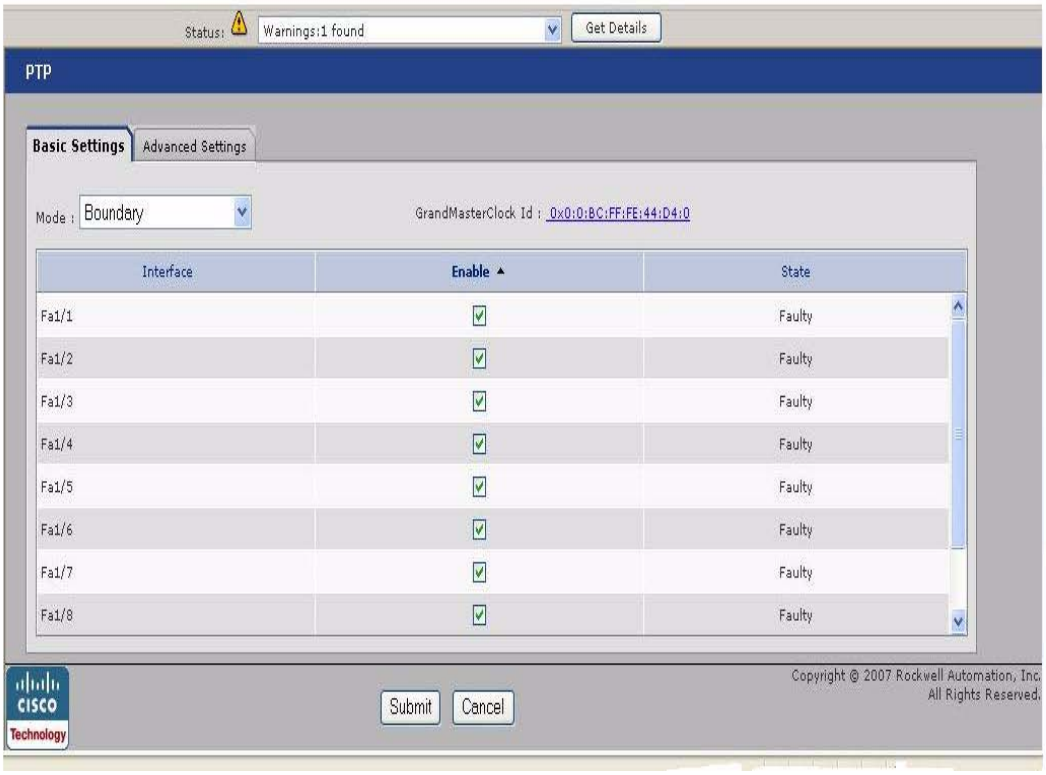
  This mode can eliminate the effects of latency fluctuations. Because jitter and errors can accumulate in cascaded topologies, this mode should be used only for networks with less than 4 layers of cascaded devices.

  In Boundary mode, one or more switch ports can be PTP-enabled.

Set the Synchronization Clock Mode

Follow this procedure to set the Synchronization Clock mode.

1. Click Configure>PTP from the Device Manager Web interface.



2. Select Boundary or Transparent mode.

In This Mode	The Switch
Boundary	This is not the preferred mode.
End-to-End Transparent	Synchronizes all switch ports with the grand master clock using the IEEE 1588 V 2 End-to-End Transparent clock mechanism.

3. Make sure the appropriate port is enabled (Enable checkbox selected).

   By default, PTP is enabled on all the Fast Ethernet and Gigabit Ethernet ports on the base switch module. Only the ports on the base switch module are PTP-capable. The switch expansion modules do not support PTP.

   In end-to-end transparent mode, all switch ports are PTP-enabled. In boundary mode, one or more switch ports can be PTP-enabled. You can enable or disable PTP on a per-port basis.

4. Check the synchronization state on the switch port.

In This Mode	The Switch Port Can Be	Description
Boundary	Listening	The switch port is waiting while a parent or grand master clock is selected.
	Pre-master	The switch port is transitioning to change to Master state.
	Master	The switch is acting as a parent clock to the devices connected to that switch port.
	Passive	The switch has detected a redundant path to a parent or grand master clock. For example, two different switch ports claim the same parent or grand master clock. To prevent a loop in the network, one of the ports changes to Passive state.
	Uncalibrated	The switch port cannot synchronize with the parent or grand master clock.
	Slave	The switch port is connected to and synchronizing with the parent or grand master clock.
	Faulty	PTP is not operating properly on that switch port.
	Disabled	PTP is not enabled on the switch port.
End-to-End Transparent	Not Faulty	The switch port is operating properly.
	Faulty	The switch port is not operating properly.
	Faulty (ptp is disabled)	PTP is not enabled on the switch port.

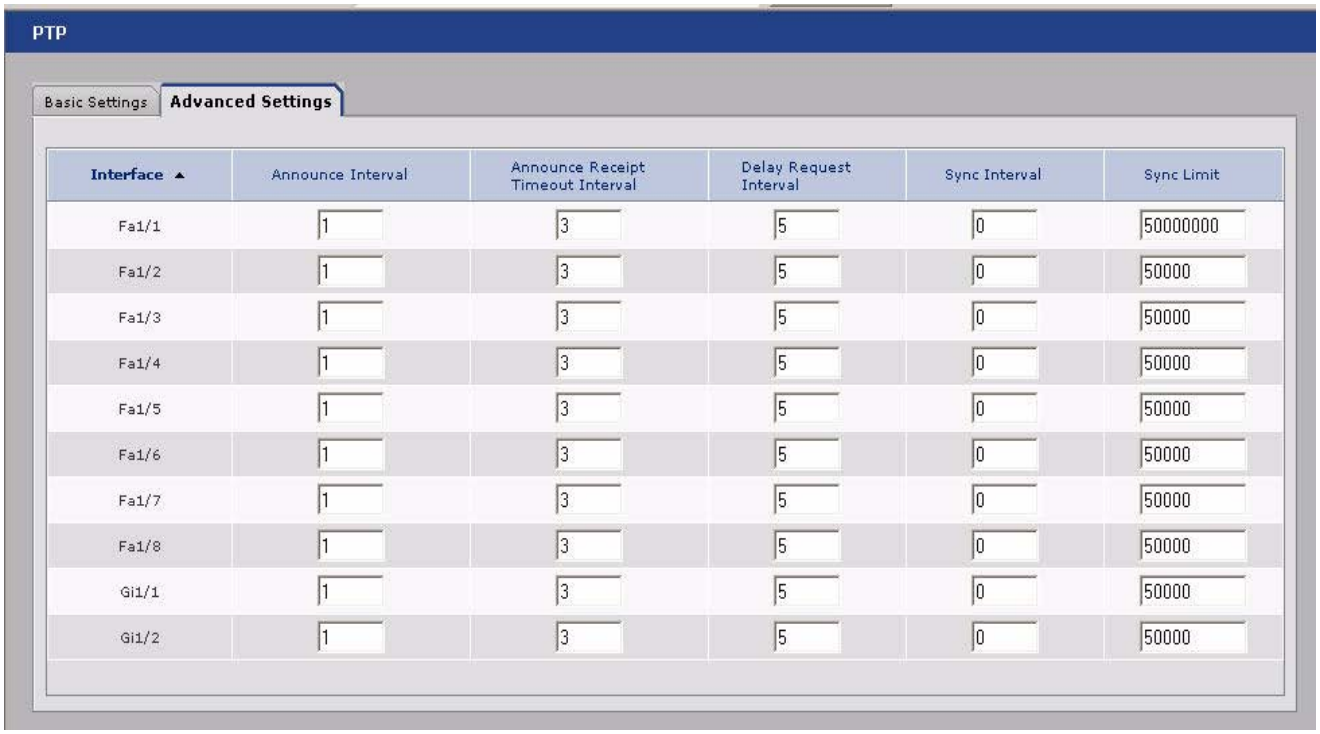
Change the PTP Timing Message Settings

Use the PTP dialog box to change the timing message settings if the switch is in Boundary mode.

1. Choose Configure>PTP from the Device Manager Web interface menu.
2. Choose Boundary mode from the Mode pull-down box.
3. Click the Advanced Settings tab.

4. Enter PTP Timing Message settings, as appropriate.

IMPORTANT When changing the PTP timing message settings, remember that the system will not operate properly unless all devices in the system have the same values.


PTP
Basic Settings
Advanced Settings
Interface
Announce Interval
Announce Receipt Timeout Interval
Delay Request Interval
Sync Interval
Sync Limit
Fa1/1 1 3 5 0 50000000
Fa1/2 1 3 5 0 50000
Fa1/3 1 3 5 0 50000
Fa1/4 1 3 5 0 50000
Fa1/5 1 3 5 0 50000
Fa1/6 1 3 5 0 50000
Fa1/7 1 3 5 0 50000
Fa1/8 1 3 5 0 50000
Gi1/1 1 3 5 0 50000
Gi1/2 1 3 5 0 50000

PTP Timing Message Settings

Setting	Description
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch number (1), and the specific port number. For example: Fa1/1 is Fast Ethernet port 1 on the base switch.
Announce Interval	The time interval for sending announce messages: • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds The default is 1 (2 seconds).
Announce Receipt Timeout Interval	The number of announce intervals that must pass without receipt of an announce message from the grand master clock before the switch selects a new grand master clock. The number can be from 2…10. The default is 3.

PTP Timing Message Settings

Setting	Description
Delay Request Interval	The time interval recommended to connected devices to send delay request messages when the switch port is in the master state: • **-1** means half second • **0** means 1 second • **1** means 2 seconds • **2** means 4 seconds • **3** means 8 seconds • **4** means 16 seconds • **5** means 32 seconds • **6** means 64 seconds The default is 5 (32 seconds).
Sync Interval	The time interval for sending synchronization messages: • **-1** means half second • **0** means 1 second • **1** means 2 seconds The default is 0 (1 second).
Sync Limit	The maximum clock offset before PTP attempts to reacquire synchronization. The value can be from 50…500,000,000 nanoseconds. The default is 50,000 nanoseconds. We recommend against setting the sync limit below the default (50,000 nanoseconds). Use values below 50,000 nanoseconds only in networks with a very high-precision grand master clock. These networks would have a critical need to keep very sensitive devices synchronized.

5. Click Submit.

Configure REP Segments

Use the REP window to configure REP segments and to display the REP segments configured on the switch.

1. To create a REP segment, set a segment ID and port type on the desired ports.

2. To display this window, choose Configure > REP from the Device Manager Web interface.

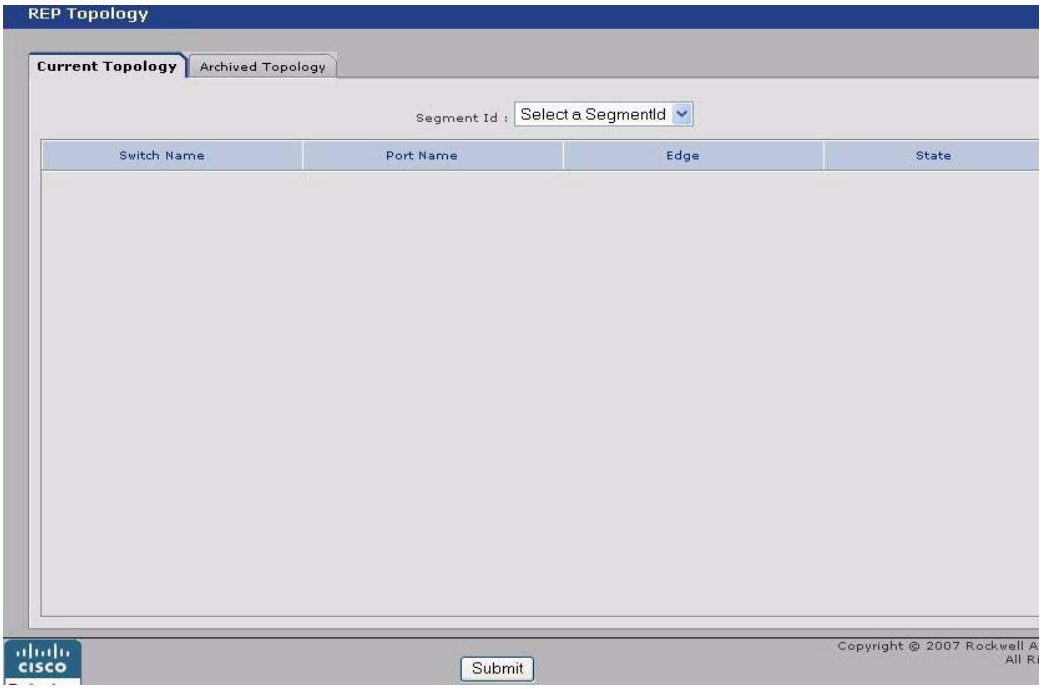
3. Enter these settings.

Setting	Description
REP Admin VLAN	The administrative VLAN. The range is 2…4094. The default is VLAN 1. REP ports are assigned to the same REP Admin VLAN. If the REP Admin VLAN changes, all REP ports are automatically assigned to the new REP Admin VLAN.
Interface	The number of the switch port, including port type (such as Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base switch number (1), and the specific port number. For example: Fa1/1 is Fast Ethernet port 1 on the base switch.
Segment ID	The ID of the segment. The segment ID range is from 1…1024. If no segment ID is set, REP is disabled.

Setting	Description
Port Type	The REP port type of the port can be: Primary, Edge, Transit, No-neighbor Primary, No-neighbor, and None. The default is None. Following are Port Type definitions: • Primary: This port is a primary edge port. This port always participates in VLAN load balancing in the REP segment. • Edge: This port is a secondary edge port. It also participates in VLAN load balancing in the REP segment. • Transit: This port is a non-edge port in the REP segment. • No-Neighbor Primary: This port is a primary edge port connected a non-REP switch. • No-Neighbor: This port is a secondary edge port connected to a non-REP switch. • The no-neighbor edge ports contain all properties of regular edge ports. These ports allow construction of a REP ring containing a switch that does not support REP protocol. • None: This port is not part of the REP segment. You must configure two edge ports on each REP segment, a primary edge port and a port to act as a secondary edge port. REP ports follow these rules: • If only one port on a switch is configured in a segment, the port should be an edge port. • If two ports on a switch belong to the same segment, both ports must be edge ports, or both ports must be regular segment ports. • If two ports on a switch belong to the same segment and one is configured as an edge port and one as a regular segment port (a misconfiguration), the edge port is treated as a regular segment port.
STCN Interface	Configure segment topology change notices (STCNs) for a port. The default is None. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN Segment	Configure STCNs to a segment ID. The default is a blank field. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.
STCN STP	Configure STCNs to a STP network. The default is an unchecked check box. TCNs are used within the segment to notify REP neighbors of topology changes. At the edge of the segment, REP can propagate the notification to the STP or to the other REP segments.

4. To review the REP topology for one or all network segments, choose Monitor>REP Topology from the Device Manager Web interface.

   You see the REP Topology dialog box.



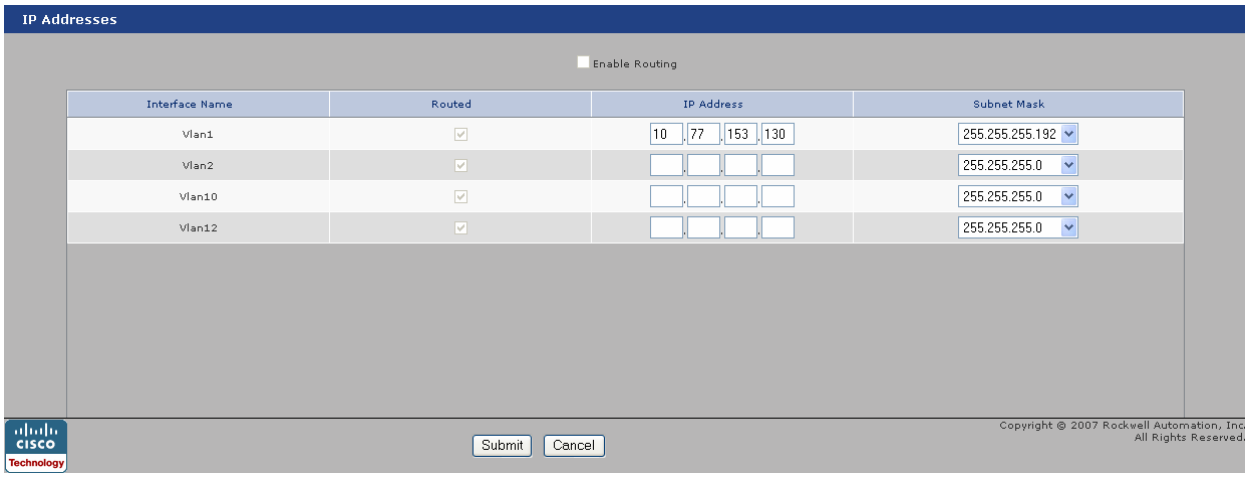
Configure IP Addresses

Use the Device Manager Web interface to configure IP addresses for VLANs.

Assign IP Addresses to VLANs

If the switch is operating as a DHCP server, the devices in a VLAN receive IP addresses from the DHCP IP address pool in the same subnet as the VLAN IP address.

Use the IP Addresses dialog to assign IP addresses to VLANs. Choose Configure > IP Addresses from the Device Manager Web interface.



Enable Static Routing (Stratix 8300 Switches Only)

The Device Manager Web interface lets you route information across VLANs and ports.

Route Across VLANs

You can use the IP Addresses tab to route between two VLANs connected to the switch. VLANs must have IP addresses assigned directly to them to allow communication to other VLANs.

To route across VLANs, define the VLAN, IP address, and subnet mask. Before configuring the routing table, you must first configure all VLANs. Refer to Configure VLANs on page 69.

Use the IP Addresses dialog to route across VLANs.

1. Choose Configure > IP Addresses from the Device Manager Web interface.

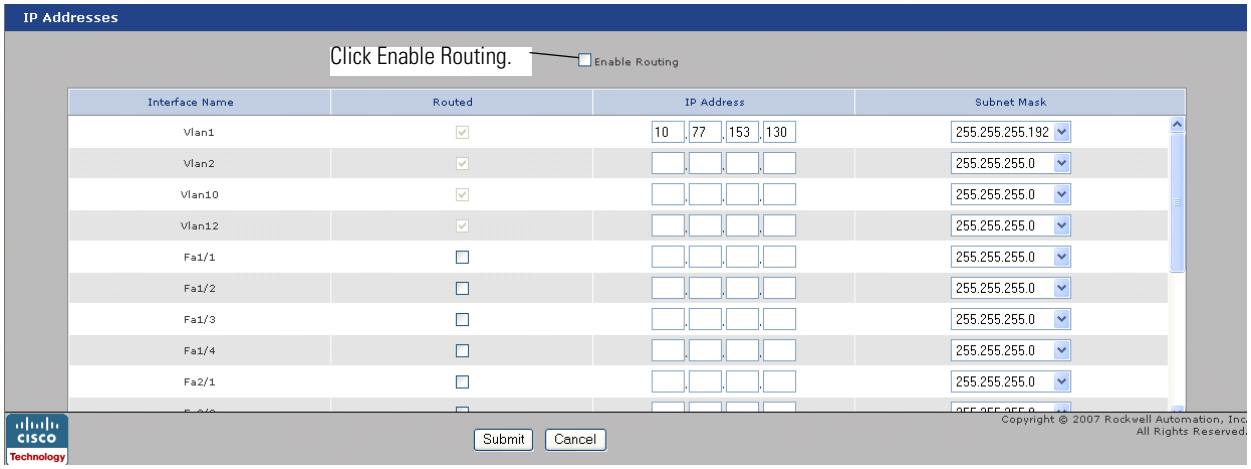
2. Assign a unique IP address and subnet mask for each VLAN.
3. Select Enable Routing.

Route Across Ports

You can also route information across ports that are on different VLANs within the Stratix 8300 switch.

To route across ports, use the IP Addresses dialog to enable static routing.

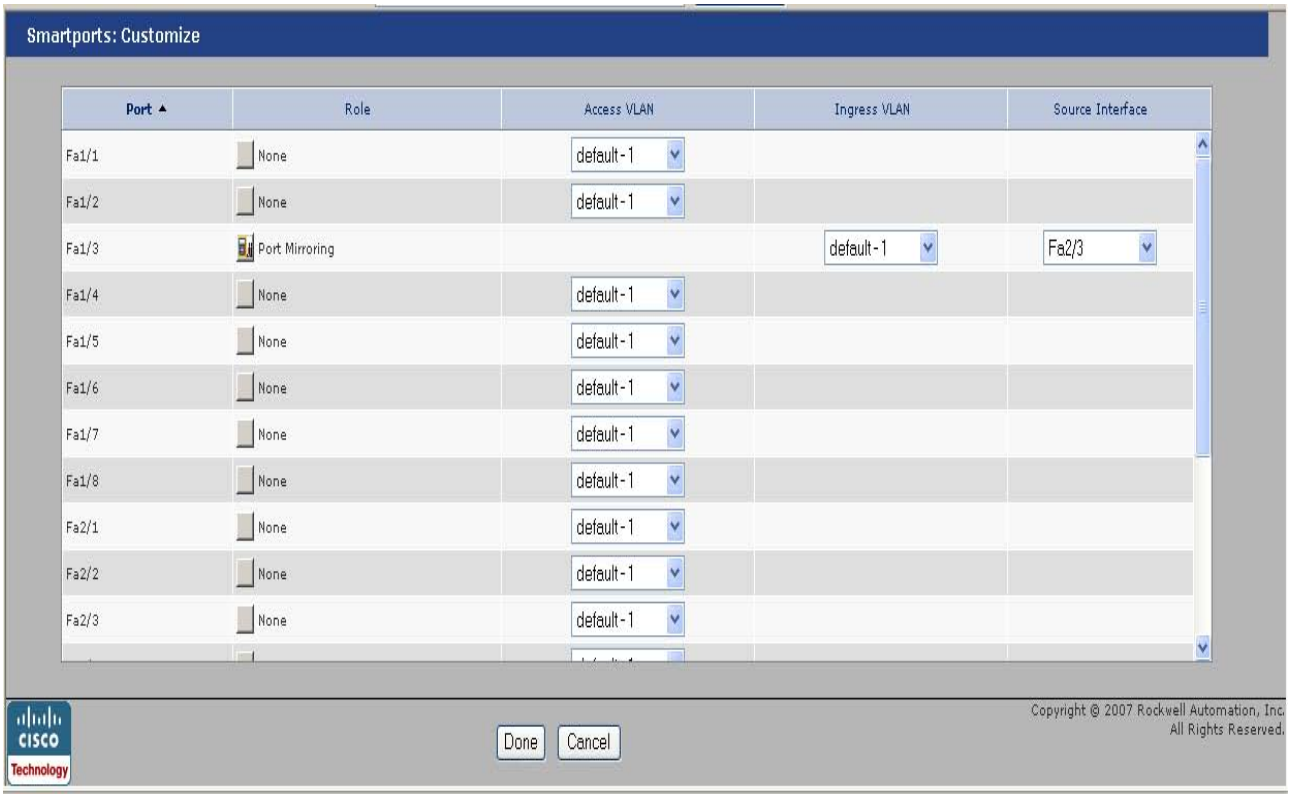
1. Choose Configure > IP Addresses from the Device Manager Web interface.
2. Select the box for each port to be routed.
3. Assign a unique IP address and subnet mask.
4. Select Enable Routing



Configure Port Mirroring

To enable port mirroring, follow this procedure.

1. From the Device Manager Web interface, choose Configure>Smartports.



2. Select the port mirroring role.
3. Apply the port that will be used for as the monitoring port.
4. Click Customize to link the port that will be mirrored (source interface and VLAN) to the monitoring port.

TIP Only one port on the switch can be monitored at a time.

Dashboard Dialog Box

Use the dashboard to monitor switch status and performance. The dashboard is displayed when you start the Device Manager Web interface.

TIP

The Dashboard gauges and graphs are like the graphs on the Trends dialog box. The Dashboard displays the instantaneous status, while the Trends graphs displays the historical status. By using them together, you can gather the detailed conditions of the switch and its ports. For information about the Trends graphs, see the Trends Graphs section on page 98.

The Front Panel view status indicators and the Status field also provide information for monitoring the switch and its ports.

Switch Information

The Switch Information area on the Dashboard displays this information about the switch, as described in the following table.

Field	Description
Host Name	The name (Host Name) of this switch configured during the initial setup. If no name was provided, this field displays the default name, Switch.
IP Address	The IP address of this switch configured during the initial setup.
MAC Address	The MAC address of this switch. This information cannot be changed.
Product ID	The model of this switch. This information cannot be changed.
CIP Revision	The switch's firmware revision, as reported by the CIP protocol object. This information cannot be changed.
CIP Serial No	The serial number of this switch. This information cannot be changed.
Hardware Rev	The hardware version of the switch. This information cannot be changed.
Software	The Cisco IOS release that this switch is running. This information is updated when you upgrade the switch firmware.
Contact	The name of the person who is the administrative contact for this switch. This information is set from the SNMP dialog box.
Location	The location of this switch. This information is set from the SNMP dialog box.

Bandwidth Used Gauge

The Bandwidth Used gauge shows the total percentage of the switch bandwidth being used. Each bar in the gauge represents 10%, and does not show increments that are less than 10%. The gauge does not show total bandwidth under 5%.

Data is collected at each 60-second system refresh. The Bandwidth Used gauge changes as the switch experiences the network activity from devices sending data through the network. As network activity increases, so does contention between devices to send data through the network. As you monitor utilization on the switch, note whether the percentage of usage is what you expect during that given time of network activity. If utilization is high when you expect it to be low, perhaps a problem exists.

As you monitor the switch, note if the bandwidth utilization is consistently high. This can mean there is congestion in the network. If the switch reaches its maximum bandwidth (above 90% utilization) and its buffers become full, it begins to discard the data packets that it receives. Some packet loss in the network is not considered unusual, and the switch is configured to help recover lost packets (such as by signaling to other devices to resend data). However, excessive packet loss can create packet errors, which can degrade overall network performance.

To reduce congestion, consider segmenting the network into subnetworks that are connected by other switches or routers. Look for other causes, such as faulty devices or connections, that can also increase bandwidth utilization on the switch.

Packet Error Gauge

The Packet Error gauge shows the total packet error percentage for the switch. Each bar in the gauge represents 10% and does not show increments that are less than 10%. The gauge does not show total packet errors under 5%.

Data is collected at each 60-second system refresh. The packet-error percentage is calculated by comparing two values:

- the total number of packets that are sent and received.
- the total number of packets with errors that are sent and received.

If the packet-error percentage is high (that is, above 10%), the switch bandwidth utilization might also be too high (a sign that the network is congested). Other causes for packet errors are faulty cabling and port misconfigurations, such as a duplex mode mismatch. These problems can cause network users to experience intermittent connectivity or loss of connectivity to the network resources (such as servers and printers) or to the Internet. Excessive collisions can cause transmission delays. For example, users might experience excessive delays in sending or receiving information through the network.

The Port Statistics dialog box displays some of the types of packet errors collected by the switch. The type of packet error can help you to identify a more precise cause for some network problems. Refer to Port Statistics on page 101 for more information.

Error	Description
Runt packets	Packets that are smaller than the allowed min size (less than 64 bytes).
Giant packets	Packets that are larger than the allowed maximum size (more than 1518 bytes).
Cyclic redundancy checksum (CRC) errors	Errors generated by the originating LAN station or far-end device do not match the checksum calculated from the data received. On a LAN, this usually means noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or of a station sending bad data.
Overrun packets	Packets that the receiving device was unable to receive.
Frame packets	Packets received because of a CRC error and a noninteger number of octets. On a LAN, this is usually the result of collisions or a malfunctioning Ethernet device.
Ignored packets	Packets that the interface ignores because the interface hardware is low on internal buffers. These buffers are different than the system buffers. Broadcast storms and bursts of noise can cause the ignored count to increase.

Temperature Status

The thermometer graphic displays this information.

OK	Green	Switch internal temperature is within the acceptable temperature range.
Faulty	Red	Switch internal temperature is above the upper temperature threshold.

For information about the switch temperature range and the operating environment guidelines, see the Stratix 8000 Ethernet Managed Switches Installation Instructions, publication 1783-IN005.

Port Utilization and Port Errors Graphs

You can see the following information on port performance:

- Port Utilization Graph: Displays the received utilization (blue) and sent utilization (purple) on each port.

  As you monitor the usage on the ports, note whether the percentage is what you expect during that given time of network activity. If usage is high when you expect it to be low, a problem might exist.

  Bandwidth allocation can also be based on whether the connection is operating in half-duplex or full-duplex mode.

- Port Errors Graph: Displays the total percentage of errors on each port.

  These are some of the reasons for errors received on or sent from the switch ports:

  – Bad cable connection
  – Defective ports
  – Software problems
  – Driver problems

Data is collected at each 60-second system refresh. Refer to Trends Graphs on page 98 for a graph that shows per-port patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days).

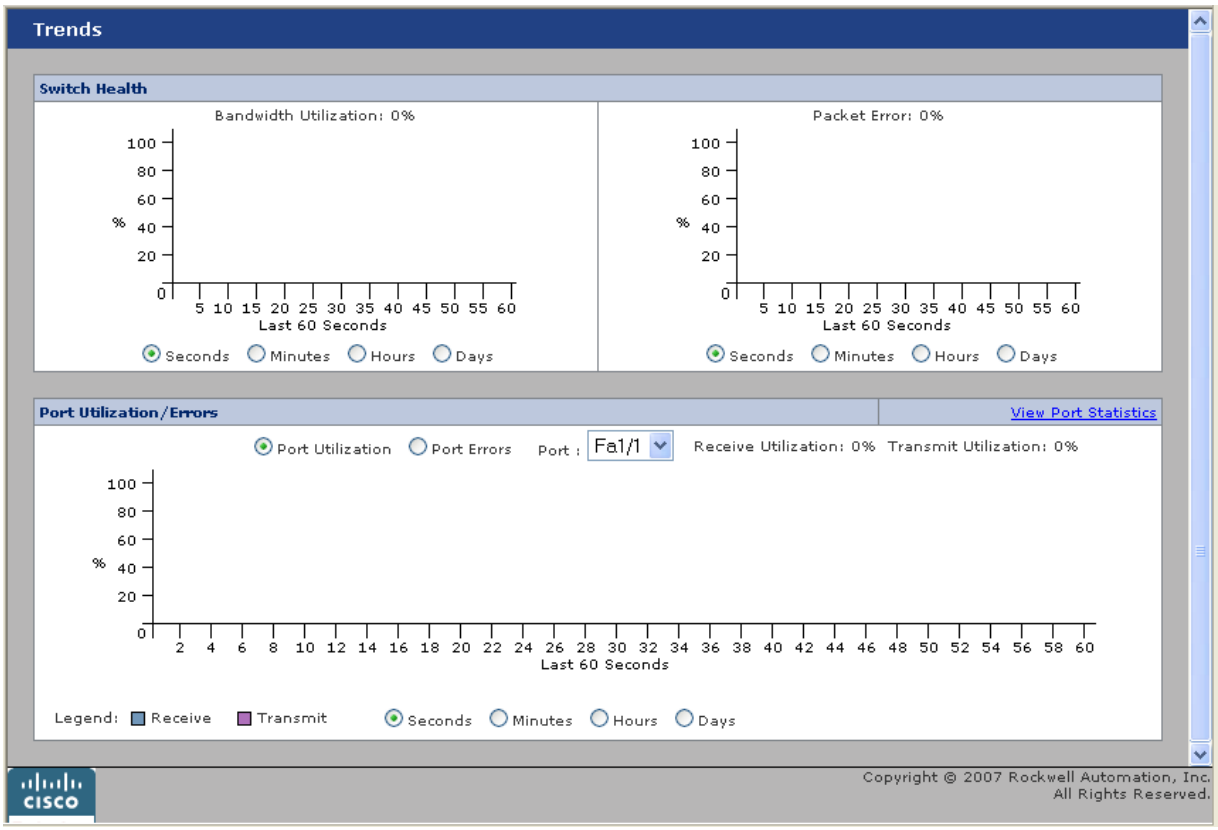
Refer to Port Statistics on page 101 for details on the specific port errors detected on each port.

Trends Graphs

Use the Trends dialog box to display the historical trends graphs. Use these graphs to display the switch bandwidth, the port usage, and the percentage of packet errors detected by the switch. You can display the data in increments of seconds, minutes, hours, and days. The level of detail displayed from these graphs can help you to analyze traffic patterns and to identify problems with the switch and individual ports.

TIP If you are using the trends graphs to monitor the switch status over time, do not end your Device Manager Web interface session.

To display the Trends dialog box choose Monitor>Trends. You can also click the View Trends link from Dashboard.


Trends
Switch Health
Bandwidth Utilization: 0%
Packet Error: 0%
%
100
80
60
40
20
0
5 10 15 20 25 30 35 40 45 50 55 60
Last 60 Seconds
Seconds Minutes Hours Days
Port Utilization/Errors
View Port Statistics
Port Utilization Port Errors Port : Fa1/1 Receive Utilization: 0% Transmit Utilization: 0%
2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 50 52 54 56 58 60
Legend: Receive Transmit
cisco
Copyright © 2007 Rockwell Automation, Inc.
All Rights Reserved.

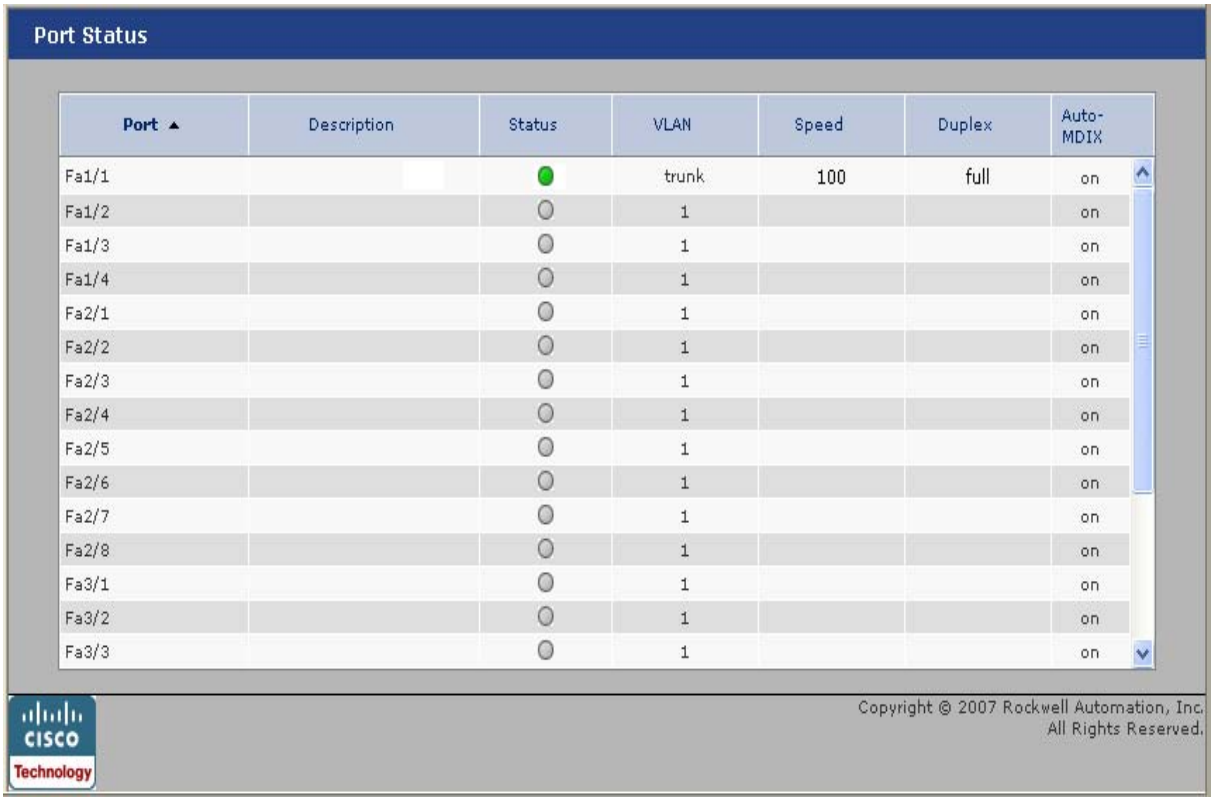
The Trends dialog box displays these graphs.

Graph	Description
Bandwidth utilization graph	The Bandwidth Utilization graph shows the same information as the Bandwidth Used gauge on the Dashboard, but the graph can show the bandwidth usage patterns over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). This graph also marks the highest peak reached. The default is 60 seconds. If you see sharp increases in switch usage, use this graph to determine when unusual peaks in network usage occur.
Packet error graph	The Packet Error graph shows the same information as the Packet Error gauge on the Dashboard, but the graph can show the percentage of packet errors collected over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. Use this graph to audit the affects that connected devices have on the switch performance or the network. For example, if you suspect that a connected device is sending error packets, you can verify if the data on the graph changes when you disconnect and reconnect the suspected device.
Per-port utilization and per-port errors graphs	The Port Utilization and Port Errors graphs on the Trends dialog box show the same information as the Port Utilization and Port Errors graphs on the Dashboard, but the graphs on the Trends dialog box can show the usage patterns of a specific port over incremental instances in time (by 60 seconds, 60 minutes, 24 hours, or 14 days). The default is 60 seconds. To display the trends for a specific port, choose a port from the Port list. Use these graphs to observe the performance of a specific port. For example, if a network user is having intermittent network connectivity, use the Port Utilization graph to observe the traffic patterns on the port to which the user's PC is connected, and use the Port Errors graph to see if the port is receiving or sending error packets.

Port Status

If the switch has link issues, such as traffic that is not being received on a switch port, use the Port Status dialog box to verify that the port settings are correct. You should also verify the settings of switch port before connecting a device to it.

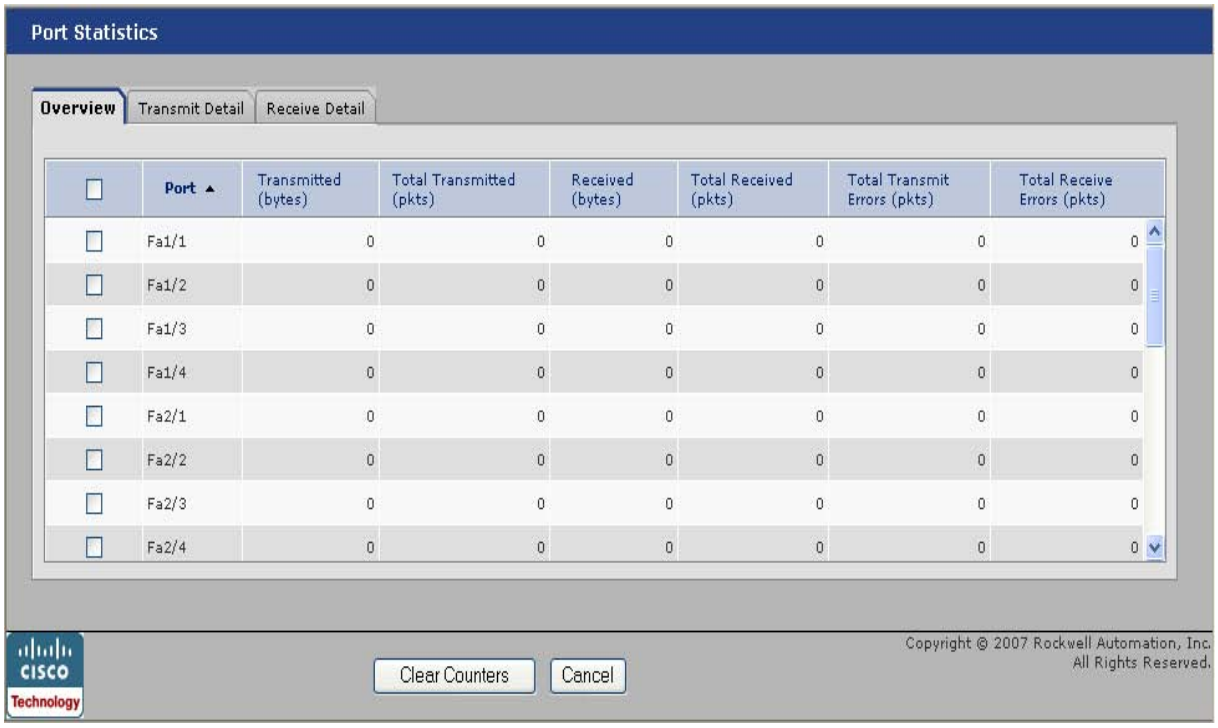
To display this dialog box, choose Monitor>Port Status from the Device Manager Web interface menu. See the Device Manager Web interface online help for additional information and procedures.



Port Statistics

The Port Statistics dialog box displays the statistics for data sent and received by the switch ports since the switch was last powered on, was restarted, or since the statistics were last cleared.

To display this dialog box, choose Monitor>Port Statistics from the Device Manager Web interface. See the Device Manager Web interface online help for additional information and procedures.



The types of port statistics collected and displayed are grouped under these tabs on the Port Statistics dialog box on the Device Manager Web interface:

- Overview tab: Use this tab to display the specific numbers of error packets received on and sent from the port, which is a level of detail that is not available from the Dashboard graphs.

  The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity.

- Transmit Detail tab: Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets sent from each port.
  – Detailed statistics of errors sent to each port.

  If a port is sending an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal or if it could mean a problem.

- Receive Detail tab: Use this tab to troubleshoot unusual changes in network traffic. This tab displays these statistics:

  – Unicast, multicast, and broadcast packets received on each port.
  – Detailed statistics of errors received on each port.

  If a port is receiving an unusually high amount of traffic (such as multicast or broadcast packets), monitor the connected device to see if this traffic pattern is normal for the connected device or if it could mean a problem.

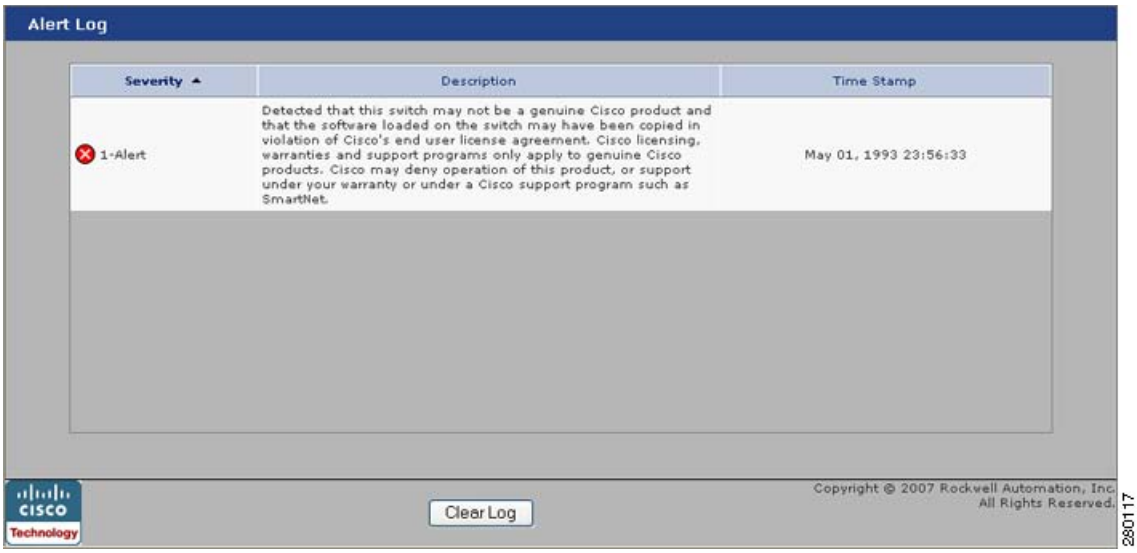
  For detailed descriptions of each statistics field, refer to the Device Manager Web interface online help.

Alert Log

The Alert Log dialog box displays switch problems that happened since the log was last cleared. The problems are issues that should be or have already been solved.

TIP Use the Alert Log with the Status field on the Front Panel view.

To display the Alert Log, choose Monitor>Alert Log from the Device Manager Web interface menu.


Alert Log
Severity
Description
Time Stamp
1-Alert
Detected that this switch may not be a genuine Cisco product and that the software loaded on the switch may have been copied in violation of Cisco's end user license agreement. Cisco licensing, warranties and support programs only apply to genuine Cisco products. Cisco may deny operation of this product, or support under your warranty or under a Cisco support program such as SmartNet.
May 01, 1993 23:56:33
Clear Log
Copyright © 2007 Rockwell Automation, Inc. All Rights Reserved.
290117

Click Clear Log to acknowledge that you have read the alerts. Clicking Clear Log does not resolve the issue.

Use the Diagnostic Test dialog box to generate a diagnostics report to resolve the issues detected by the switch.

The Alert Log includes this information.

Issue	Description
Severity Level	A single-digit code (0…5) that reflects the severity of the problem. The lower the number, the more serious the condition and the need to take action. Emergency (0)—The switch is unusable. Alert (1)—The switch requires immediate action. Critical (2)—The switch has a critical condition. Error (3)—The switch has an error condition. Warning (4)—The switch has a warning condition. Notifications (5)—The switch is operating normally but has a significant condition.
Description	The description of the problem, including the port on which the problem was detected.
Time Stamp	The date and time of the refresh cycle during which the problem was last detected.

CIP Status

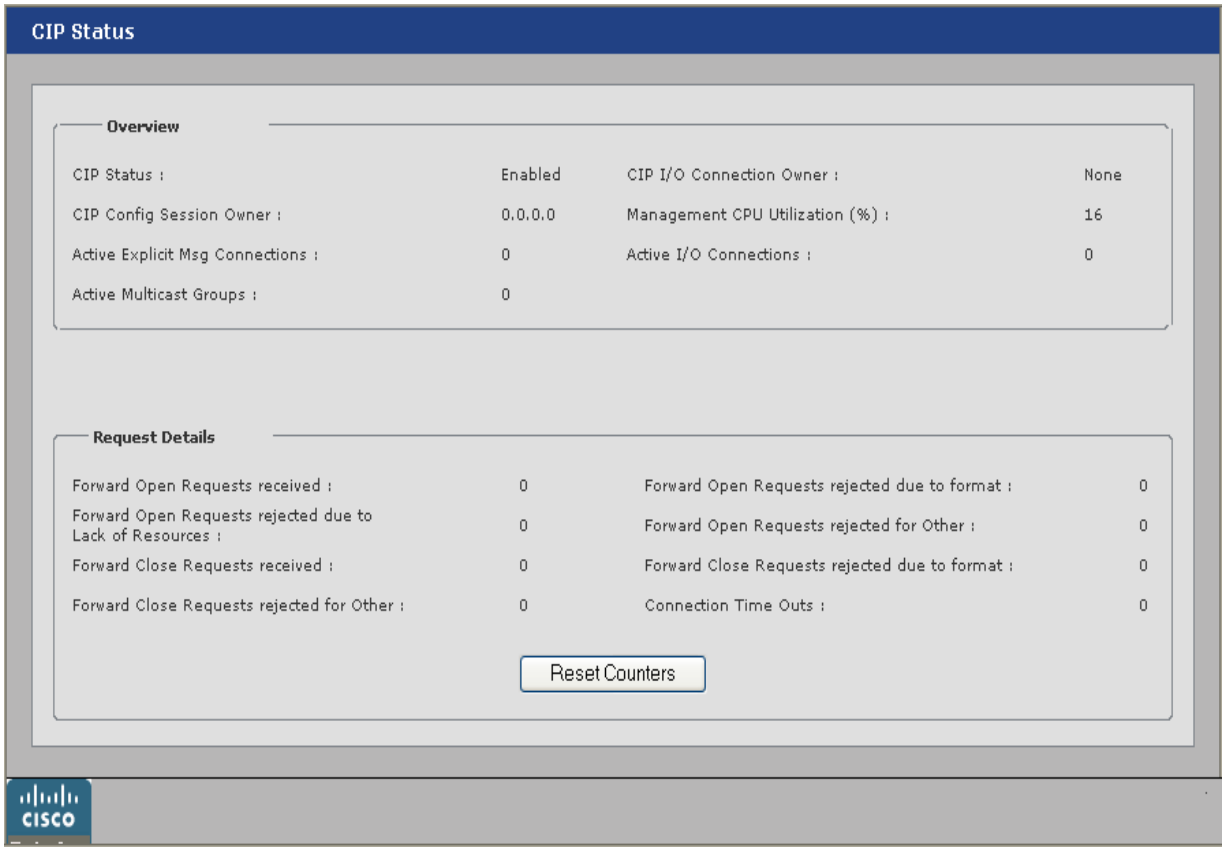
Control and Information Protocol (CIP) is an application layer messaging protocol used by various industrial automation and control devices to communicate as part of a control system. CIP is the application layer for the EtherNet/IP network. Stratix 8000 and Stratix 8300 switches contain an EtherNet/IP server that enables the switch to be part of the industrial automation and control system for basic management and monitoring.

The CIP Status dialog box displays information about CIP status (Overview field) and statistics (Request Details field) since the switch was last powered on, was restarted, or the counters were last reset.

To troubleshoot an issue, reset the CIP counters, and see if the counters show that the issue still exists.

IMPORTANT Except for Active Multicast Groups, all other categories are related to the CIP server in the switch, that is, pertaining to CIP traffic specifically directed to the switch as a CIP target device. They do not refer to CIP (EtherNet/IP) traffic flowing through the switch among various CIP controllers, HMI devices, configuration tools, or other CIP target devices, such as drives, I/O modules, motor starters, sensors, and valves.

To display this dialog box, choose Monitor>CIP Status from the Device Manager Web interface menu.



Overview status

Field	Description
CIP Status	The state of the CIP protocol (Enabled or Disabled).
CIP I/O Connection Owner	The IP address of the device to and from which application-specific I/O output data is sent and received.
CIP Config Session Owner	The IP address of the device controlling the CIP configuration session.
Management CPU Utilization (%)	Percentage of the Management CPU used for management functions. Switch functions have dedicated ASICs that are not impacted by management functions.
Active Explicit Msg Connections	The number of active, explicit messaging connections to the switch as a target.
Active I/O Connections	The number of active I/O connections with the switch as a target.
Active Multicast Groups	The number of multicast groups, including CIP multicast groups flowing through the switch.

Request Details Status

State	Description
Forward Open Requests Received	The number of Forward Open requests received by the switch to establish a connection with the switch.
Forward Open Requests Rejected Due to Lack of Resources	The number of Forward Open requests that failed for reasons such as insufficient memory to establish a new connection with the switch.
Forward Open Requests Rejected Due to Format	The number of Forward Open requests directed to the switch that failed because the request is not in the proper format.
Forward Open Requests Rejected For Other	The number of Forward Open requests directed to the switch that failed for reasons such as incompatible electronic keying.
Forward Close Requests Received	The number of Forward Close requests received by the switch after a connection was successfully established with the switch.
Forward Close Requests Rejected Due to Format	The number of Forward Close requests directed to the switch that failed because the request is not in the proper format.
Forward Close Requests Rejected For Other	The number of Forward Close requests directed to the switch that failed for reasons such as incompatible electronic keying.
Connection Time Outs	The number of CIP connections that timed out due to inactivity.

Upgrade the Switch Firmware

You must have access to the Internet to download switch firmware from http://www.rockwellautomation.com to your computer or network drive.

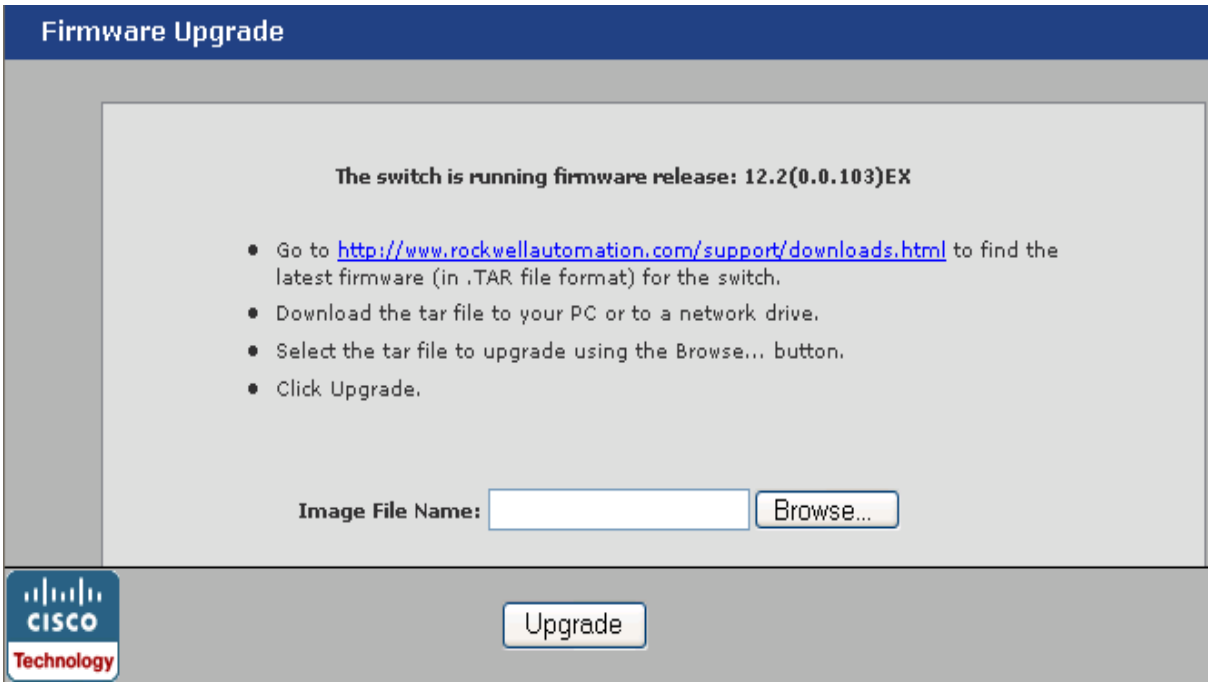
Use the Device Manager Firmware Upgrade dialog box to update the switch with the latest software changes (such as software patches) and features. From the Device Manager Web interface, you can upgrade your switches one at a time.

To display this dialog box, choose Maintenance>Firmware Upgrade from the Device Manager Web interface menu.

IMPORTANT Wait for the upgrade process to complete. Do not use or close the browser session with the Device Manager Web interface active. Do not access the Device Manager Web interface from another browser session.

When the upgrade process completes, a success message appears, and the switch automatically restarts. It might take a few minutes for the switch to restart with the new firmware.

Verify that the latest firmware version on the switch appears in the Software field in the Switch Information area of the Dashboard.


Firmware Upgrade
The switch is running firmware release: 12.2(0.0.103)EX
Go to http://www.rockwellautomation.com/support/downloads.html to find the latest firmware (in .TAR file format) for the switch.
Download the tar file to your PC or to a network drive.
Select the tar file to upgrade using the Browse... button.
Click Upgrade.
Image File Name:
Browse...
Upgrade

See the Device Manager Web interface online help for additional guidelines and procedures.

Notes:

Manage the Switch via RSLogix 5000 Software

Introduction

After you complete Express Setup, you can manage the switch by using the RSLogix 5000 software.

Topic	Page
EtherNet/IP CIP Interface	109
Add a Switch to the I/O Configuration Tree	114
Configure Module Properties	116
Connection Properties	119
General Switch Properties	120
Basic Port Properties	122
Advanced Port Properties	124
Port Thresholds (Storm Control)	128
Save and Restore Switch Configuration	130
Monitor and Reset the Switch	131
Switch Status	133
Port Status	135

EtherNet/IP CIP Interface

Stratix 8000 and Stratix 8300 switches contain an EtherNet/IP network interface. EtherNet/IP is an industrial automation network specification maintained by the Open DeviceNet Vendor Association (ODVA). It uses the Common Industrial Protocol (CIP) for its application layer, and TCP/UDP/IP for its transport and network layers. This interface is accessible via any of the switch's Ethernet ports by using the IP address of the switch.

CIP Network Connections

CIP is an object-oriented connection-based protocol that supports two basic types of messaging: Explicit and Implicit (I/O) connections. A maximum of 32 connections is available. Both connection types must use the switch password before any switch parameters can be written. The password is the same one you entered during Express Setup.

Connection	Description
Explicit messaging	Explicit messaging connections provide generic, multi-purpose communication paths between two devices. These connections are often referred to as messaging connections. Explicit messages provide the typical request/response-oriented network communication. Each request is typically directed at a different data item. Explicit messages can be used for configuring, monitoring and troubleshooting the switch. The Explicit Messaging interface is used by the RSLogix 5000 Add-on Profile for the switch.
I/O (implicit messaging)	I/O connections provide dedicated, special purpose communication paths between a producing application and one or more consuming applications. The application-specific I/O data that moves through these connections is typically a fixed, cyclical structure. The Switch supports two I/O connection choices. • Input Only • Exclusive Owner Both connections are cyclic and adjustable from 300...5000 ms. The Input Only connection contains a data structure with status information on the switch in general and specific status on each of the ports. This connection is multicast and can be shared by multiple controllers (connection originators). The Exclusive Owner connection uses the same Input data structure as the Input Only connection, but adds an Output data structure. The Output data contains a bit for each port that allows you to enable or disable each port separately. While the Input data on this connection can be shared (via multicast) by multiple controllers, only one controller may own the Output data. If a second controller attempts to open this connection, the connection will be rejected

.

IMPORTANT Because the output data is sent cyclically by the controller, it overrides any other attempt to enable or disable a port from other software tools or visualization stations.

RSLinx Software and Network Who Support

The EtherNet/IP network interface also supports the List Identity command, used by CIP-based network tools such as the RSLinx software RSWho function. RSWho enables you to locate and identify your switch on the network, using electronic data sheet (EDS) files.

To perform an RSWho, from the RSLinx software toolbar, choose Communications>RSWho.

IMPORTANT If, after performing an RSWho, you access the switch and view the Ethernet link counters, you will see the counts only for the first port (Port Gi1/1).

Electronic Data Sheet (EDS) Files

EDS files are simple text files used by network configuration tools, such as RSNetWorx for EtherNet/IP software, to help you identify products and easily commission them on a network. EDS files contain details about the readable and configurable parameters of the device. They also provide information about the I/O connections the device supports and the content of the associated data structures.

If you are using the switch in a system that does not have a Rockwell Automation Logix-based controller to monitor or control your switch, you will not be able to use the Add-on Profile (AOP) supplied with Logix controllers. You must use information from the EDS files to set up the I/O connection.

The OPC Server contained in RSLinx Classic software also uses EDS files to provide you with a selectable list of parameters when adding items (OPC Tags) to a Topic (the switch).

EDS files for the Stratix 8000 switches are included with the following software packages:

- RSLinx software, version 2.54 or later
- RSLogix 5000 software, version 17 or later
- RSNetWorx for EtherNet/IP software, version 9.0 or later

You can also obtain the EDS files in either of these two ways:

- By downloading it from http://www.rockwellautomation.com/resources/eds/.

TIP To locate a specific EDS file, do the following.

1. Select EtherNet/IP in the Network type field.
2. Enter Stratix 8000 in the Keyword field.
3. Leave the other fields with their default entries.

- Directly from the switch by using the RSLinx EDS Hardware Installation Tool.

  Follow this procedure to upload the EDS files directly from the switch over the network.

TIP Six different EDS files are supplied with the switch, one for each port count (6, 10, 14, 18, 22 and 26 ports). Regardless of the switch from which you upload EDS files, you will receive all six files and the Stratix 8000 switch icon.

1. From your computer, choose Start>Programs>Rockwell Software>RSLinx>Tools>EDS Hardware Installation Tool.
2. Click Add to launch the EDS Wizard and add the selected hardware description and associated files.

Data Accessible With CIP

The CIP interface lets you access the following information:

- Input Data via I/O Connection
  - Link Status per Port: not connected, connected
  - Unauthorized Device per Port: OK, not OK
  - Unicast Threshold Exceeded per Port: OK, exceeded
  - Multicast Threshold Exceeded on each Port: OK, exceeded
  - Broadcast Threshold Exceeded on each Port: OK, exceeded
  - Port Bandwidth Utilization per Port: value in %
  - Alarm Relay Minor: OK, tripped
  - Alarm Relay Major: OK, tripped

  - Multicast Groups Active: quantity

- Output Data via I/O Connection

  - Port Disable per port: enabled, disabled

- Other Status Data

  - Switch Internal Temperature: degrees Centigrade
  - Power Supply A present: yes, no
  - Power Supply B present: yes, no
  - Identity Info: VendorID, DeviceType, ProductCode, ProductName, Revision, SerialNumber
  - IOS Release version
  - Switch Uptime (since last reboot)
  - Management CPU Utilization: in %
  - CIP Connection Counters: open/close requests, open/close rejects, timeouts
  - Port Alarm Status per port: OK, not forwarding, not operating, excessive FCS errors
  - Port Fault Status per port: Error Disable, SFP error, native VLAN mismatch, MAC address flap condition, security violation
  - Port Diagnostic Counters per port: Ethernet Interface counters (10), Ethernet Media counters (12)

- Configuration Data (requires password)

  - IP Address Method: DHCP, static
  - IP Address, Subnet Mask, Default Gateway (all if static)
  - Host Name
  - Contact name
  - Geographic Location
  - Port Config per port: enable/disable, autonegotiate, forced speed/duplex
  - Authorized MACID per port
  - Unicast Storm Control Threshold per port: in packets per second, bits per sec, or %
  - Multicast Storm Control Threshold: in packets per second, bits per sec, or %
  - Broadcast Storm Control Threshold: in packets per second, bits per sec, or %

- Smart Port assignment per port: Role and VLAN

- Save and Restore of Switch Configuration (via File Obj)

Add a Switch to the I/O Configuration Tree

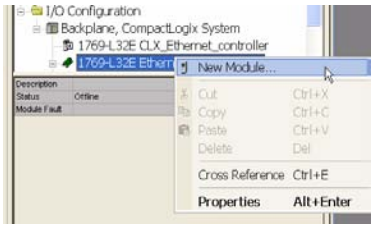
Follow this procedure to add the switch to the controller's I/O tree.

IMPORTANT These steps are required before you can go online to configure and monitor the switch.

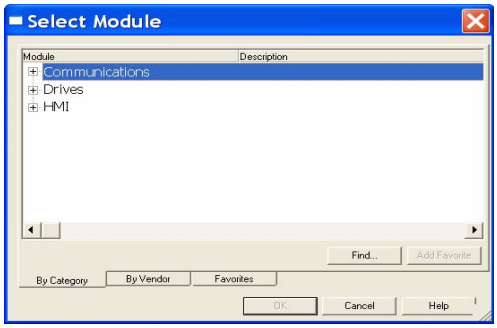
1. Open the project file for the controller that will be monitoring the switch.
2. Select the Ethernet module through which the controller will communicate with the switch.

   In this example, the switch communicates through a 1769-L32E CompactLogix EtherNet/IP controller.

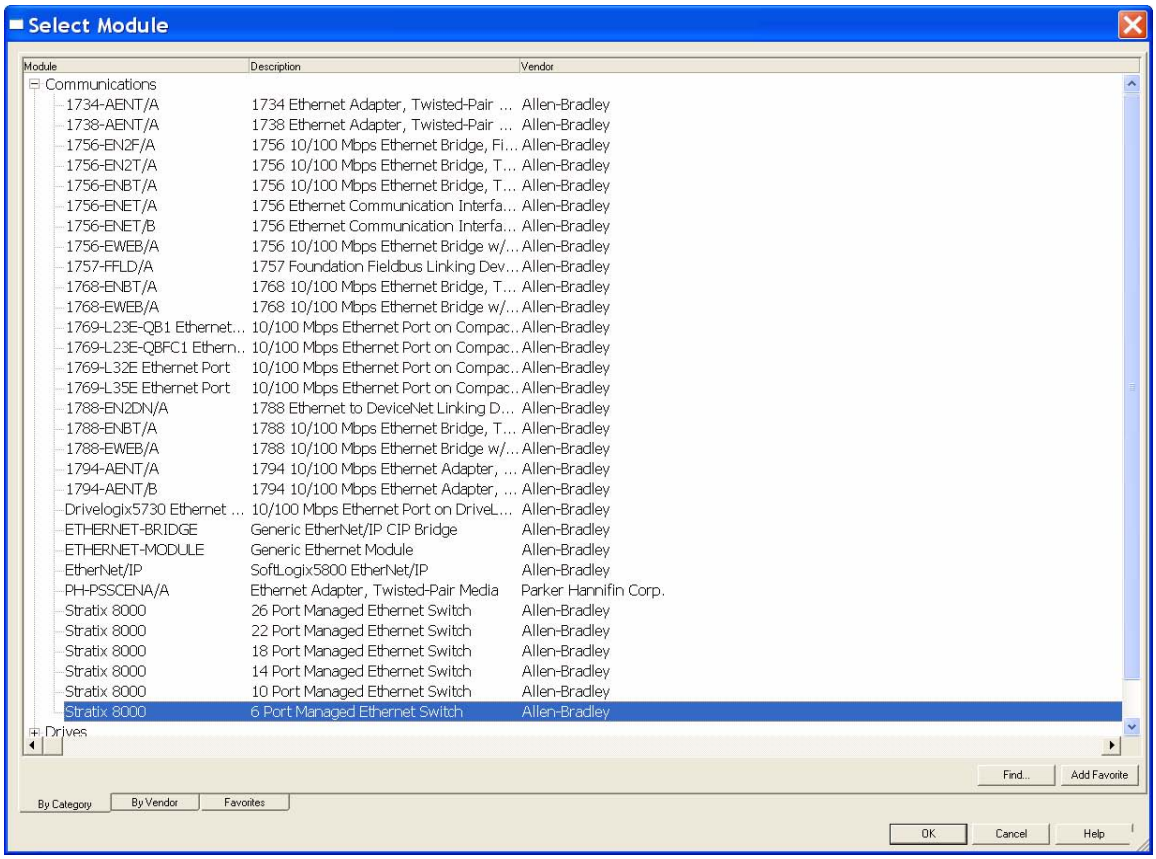
3. Add the switch to the project.
   a. Right-click the Ethernet port you created and choose New Module.



   b. Click Communications.



c. Click the + sign and scroll down until you see the switch you want to configure.


Select Module
Module
Description
Vendor
Communications
1734-AENT/A 1734 Ethernet Adapter, Twisted-Pair ... Allen-Bradley
1738-AENT/A 1738 Ethernet Adapter, Twisted-Pair ... Allen-Bradley
1756-EN2F/A 1756 10/100 Mbps Ethernet Bridge, Fi... Allen-Bradley
1756-EN2T/A 1756 10/100 Mbps Ethernet Bridge, T... Allen-Bradley
1756-ENBT/A 1756 10/100 Mbps Ethernet Bridge, T... Allen-Bradley
1756-ENET/A 1756 Ethernet Communication Interfa... Allen-Bradley
1756-ENET/B 1756 Ethernet Communication Interfa... Allen-Bradley
1756-EWEB/A 1756 10/100 Mbps Ethernet Bridge w/... Allen-Bradley
1757-FFLD/A 1757 Foundation Fieldbus Linking Dev... Allen-Bradley
1768-ENBT/A 1768 10/100 Mbps Ethernet Bridge, T... Allen-Bradley
1768-EWEB/A 1768 10/100 Mbps Ethernet Bridge w/... Allen-Bradley
1769-L23E-QB1 Ethernet... 10/100 Mbps Ethernet Port on Compac... Allen-Bradley
1769-L23E-QBFC1 Ethern... 10/100 Mbps Ethernet Port on Compac... Allen-Bradley
1769-L32E Ethernet Port 10/100 Mbps Ethernet Port on Compac... Allen-Bradley
1769-L35E Ethernet Port 10/100 Mbps Ethernet Port on Compac... Allen-Bradley
1788-EN2DN/A 1788 Ethernet to DeviceNet Linking D... Allen-Bradley
1788-ENBT/A 1788 10/100 Mbps Ethernet Bridge, T... Allen-Bradley
1788-EWEB/A 1788 10/100 Mbps Ethernet Bridge w/... Allen-Bradley
1794-AENT/A 1794 10/100 Mbps Ethernet Adapter, ... Allen-Bradley
1794-AENT/B 1794 10/100 Mbps Ethernet Adapter, ... Allen-Bradley
Drivelogix5730 Ethernet ... 10/100 Mbps Ethernet Port on DriveL... Allen-Bradley
ETHERNET-BRIDGE Generic EtherNet/IP CIP Bridge Allen-Bradley
ETHERNET-MODULE Generic Ethernet Module Allen-Bradley
EtherNet/IP SoftLogix5800 EtherNet/IP Allen-Bradley
PH-PSSCENA/A Ethernet Adapter, Twisted-Pair Media Parker Hannifin Corp.
Stratix 8000 26 Port Managed Ethernet Switch Allen-Bradley
Stratix 8000 22 Port Managed Ethernet Switch Allen-Bradley
Stratix 8000 18 Port Managed Ethernet Switch Allen-Bradley
Stratix 8000 14 Port Managed Ethernet Switch Allen-Bradley
Stratix 8000 10 Port Managed Ethernet Switch Allen-Bradley
Stratix 8000 6 Port Managed Ethernet Switch Allen-Bradley
Drives
Find...
Add Favorite
By Category
By Vendor
Favorites
OK
Cancel
Help

TIP If you do not see the switch on the list, you may need to obtain the AOP from the Rockwell Automation support website.

1. Go to http://www.rockwellautomation.com/support/.
2. Click Downloads/RSLogix 5000 I/O Modules Add-on Profiles.
3. Select the 1783-Stratix 8000 Managed Switches Add-on Profile.

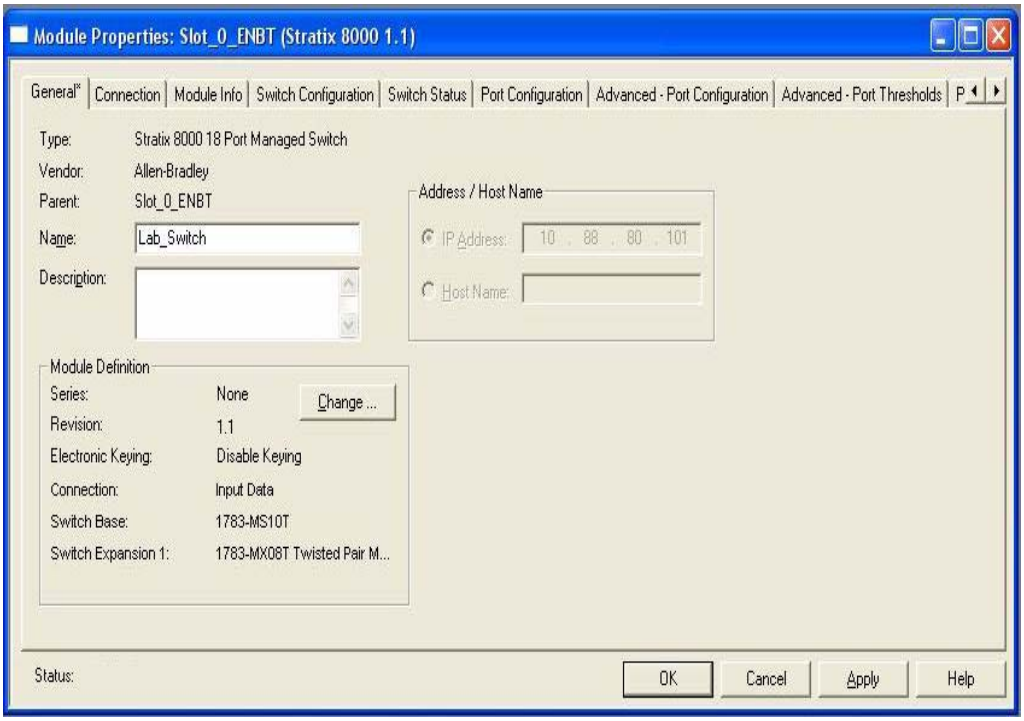
d. Click OK.

You see the Module Properties dialog box, which contains these tabs:

- General
- Connection
- Module Info
- Switch Configuration
- Switch Status
- Port Configuration
- Advanced - Port Configuration
- Advanced - Port Thresholds
- Port Status
- Save/Restore

Configure Module Properties

1. From the Module Properties dialog box, enter this information.



IMPORTANT Be sure that the IP address and host name are the same as those provided when you performed the Express Setup. In the Module Properties dialog box, you can select either IP address or host name. Only one of these two choices is enabled.

In this field	Enter
Name	A name you choose for the switch.
Description	A description that helps you remember something important about the switch.
Choose one of the following	
IP Address	The IP address you entered when you performed the Express Setup. The controller uses the IP address to communicate.
Host Name	The host name provided on initial configuration when you performed the Express Setup.The host name requires that you have a DNS server configured on the network for the controller's Ethernet interface module.

2. Click OK.

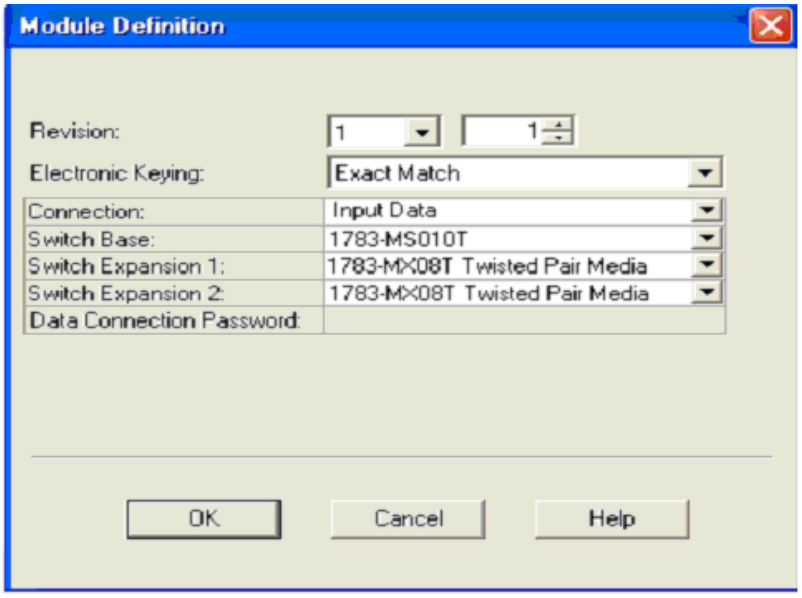
   The switch is added to the project.

3. Go online with the switch by choosing Communictions>Go online.

4. Double-click the switch to view the Module Properties dialog box.

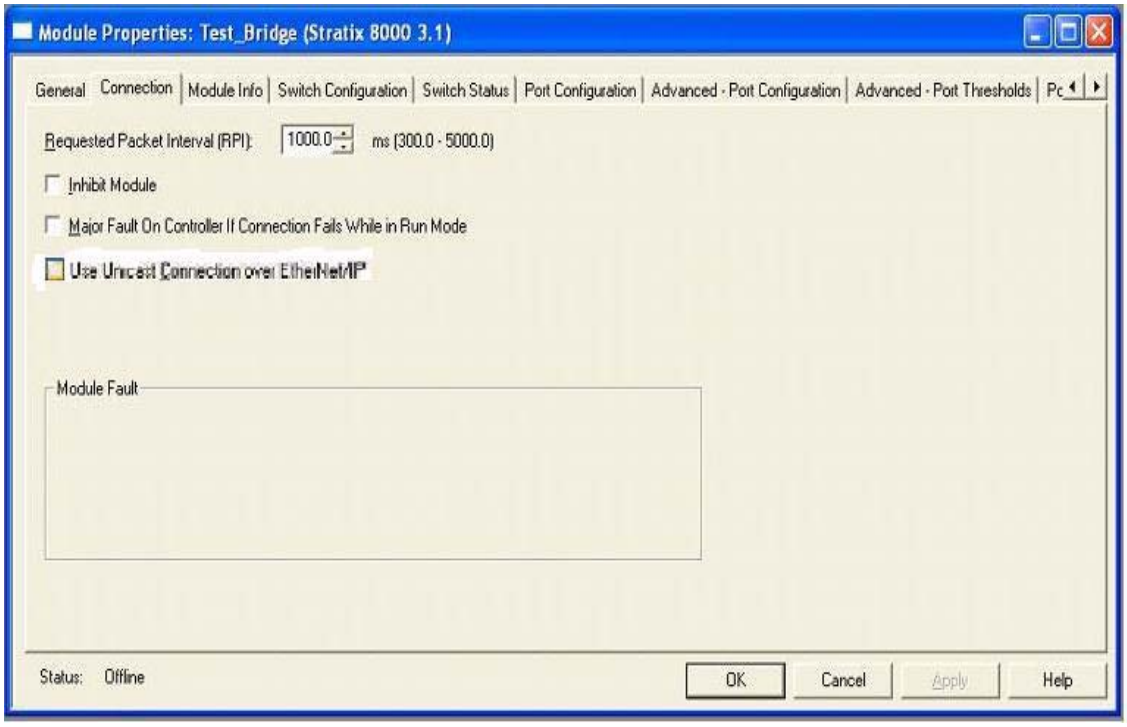
5. Click Change.

   You see the Module Definition dialog box.



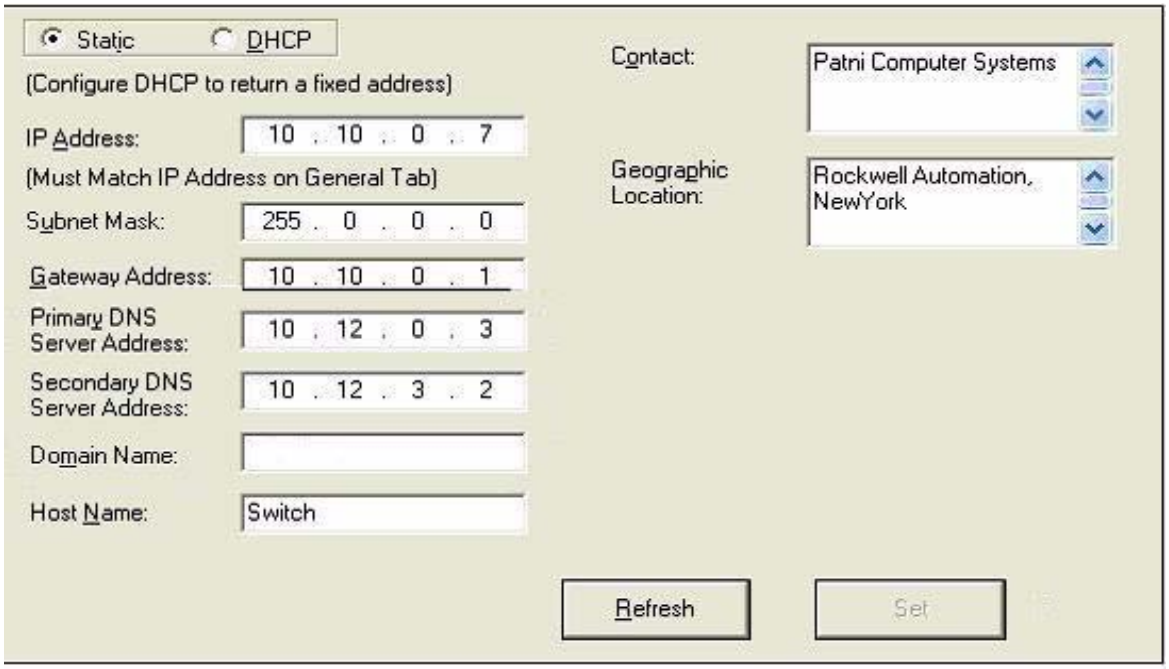
In this field	Select
Revision	The major and minor revision of the switch. Major revision: a number from 1...128. Minor revision: a number from 1...255.
Electronic Keying	• Compatible Module (default). • Exact Match. • Disable Keying.
Connection	• Input Data (default): Allows input data connection only. • Data: Allows input and output data connection. **Attention:** This selection enables output tags, which can disable ports and interrupt connections to and through the switch. You can disable a switch port by setting the corresponding bit in the output tag. The output bits will be applied every time the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied. The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using the Device Manager Web interface or the CLI, the port setting may be overridden by the output bits from the controller on the next cyclic update of the I/O connection. The output bits will always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.
Switch Base	All selections are disabled. The switch base catalog number will be displayed based on the module you selected.
Switch Expansion 1	The catalog number for the copper or fiber expansion modules you are using. Displayed for 14, 18, 22 and 26 port switches. For 14 and 18 port switches, user selection of the expansion module is allowed. For 22 and 26 port switches, Switch Expansion 1 will display 1783-MX08T. User selection of the expansion module is not allowed.
Switch Expansion 2	The catalog number for the copper or fiber expansion modules you are using. Displayed only for 22 and 26 port switches. User selection of the expansion module is allowed.
Data Connection Password	Enter the password for accessing the switch. Required for Data connection only.

Connection Properties



In this field	Values are	Comments
Requested Packet Interval (RPI)	300…5000	
Inhibit Module	Check to disable communication between the controller and the switch. Uncheck to restore communication.	
Major Fault on Controller If Connection Fails While in Run Mode	Check to have the controller create a major fault if connection fails in Run mode.	
Use Unicast Connections over EtherNet/IP	Check to use Unicast connections with the EtherNet/IP network.	
Module Fault		Displays the fault code returned from the controller (related to the switch you are configuring), and the text detailing the module fault has occurred.

General Switch Properties



Use this tab to configure the parameters for the switch configuration. You must be online to perform these configurations. In Offline mode nothing is displayed on this tab.

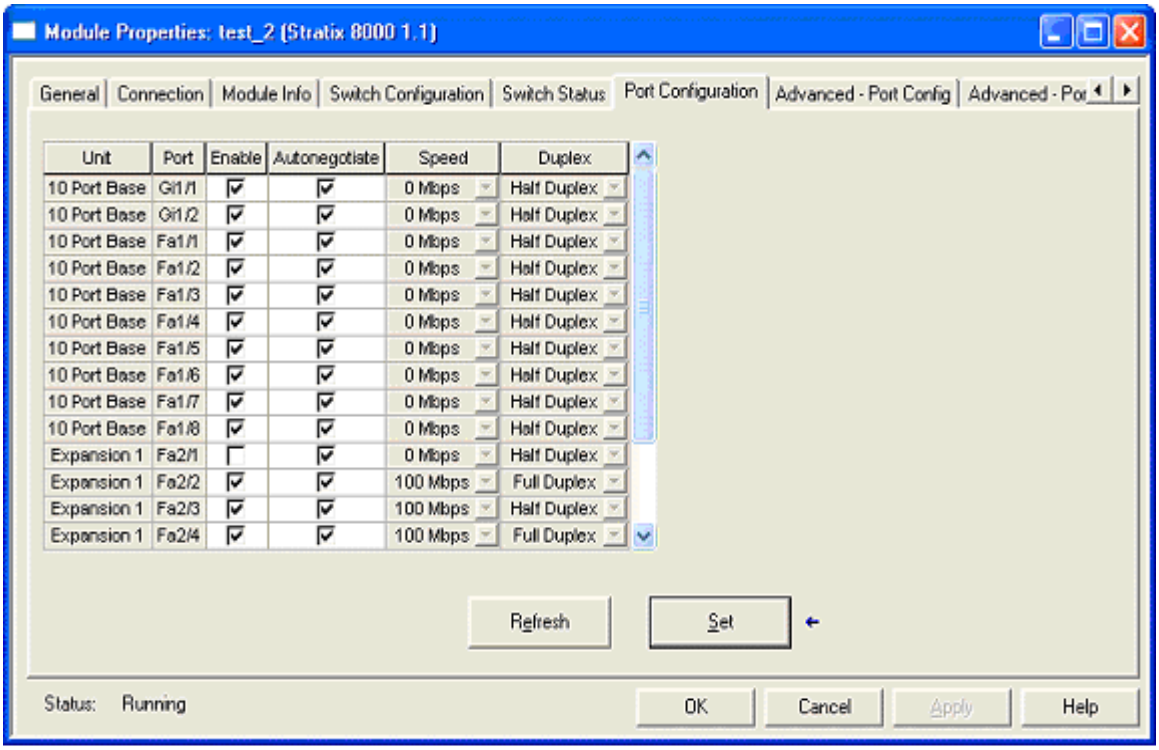
The IP address can be manually assigned (static) or it can be automatically assigned by a Dynamic Host Configuration Protocol (DHCP) server. The default is Static. We recommend that you select Static and manually assign the IP address for the switch. You can then use the same IP address whenever you want to access the switch.

- Static - Manually enter the IP address, subnet mask, and gateway.
- DHCP - The switch automatically obtains an IP address, default gateway, and subnet mask from the DHCP server. As long as the switch is not restarted, it continues to use the assigned IP information.

In this field	Values are	Comments
IP Address	N/A	This value must match the IP address on the General tab. If you reconfigure your switch with a different IP address, you may lose communication with the switch when you click Set. To correct this problem, you must go back to the Express Setup and General tab, set the new IP address, and download to the controller.

In this field	Values are	Comments
Subnet Mask	Enter the appropriate subnet mask for the switch.	The subnet mask is a 32-bit number. Set each octet between 0 and 255. The default is 255.255.255.0
Gateway Address	N/A	A gateway is a router or other network device through which the switch communicates with devices on other networks or subnetworks. The gateway IP address should be part of the same subnet as the switch IP address. The switch IP address and the default gateway IP address cannot be the same. **Attention:** Communication will be disrupted when the gateway (IP) address is changed.
Primary DNS Server Address	Enter the IP address of the primary Domain Name Server (DNS).	Set each octet between 0…255. The first octet may not be 127, or a number greater than 223
Secondary DNS Server Address	Enter the IP address of the secondary Domain Name Server (DNS).	Set each octet between 0…255. The first octet may not be 127, or a number greater than 223
Domain Name	Enter the name of the domain in which the module resides.	The domain name consists of a sequence of name labels separated by periods, such as example.com. The domain name has a 48-character limit and is restricted to ASCII letters a…z, digits 0…9, and periods and hyphens.
Host Name	Enter a name to help identify the switch when monitoring or troubleshooting a problem. This feature is optional.	The name can be up to 64 characters and can include alphanumeric and special characters (comma and dash).
Contact	Enter contact information for the switch, up to 200 characters. This feature is optional.	The contact information can include alphanumeric and special characters (dash and comma) and a carriage return.
Geographic Location	Enter a geographic location of the switch, up to 200 characters. This feature is optional.	The geographic location can include alphanumeric and special characters (dash and comma) and a carriage return.
Refresh	Click to refresh the tab with new data from the module.	This button is active on many tabs.
Set	Click to send the settings to the switch. Changes can be made within 10 minutes without the Enter Password dialog box displaying and prompting you for a password.	Changes are saved to the switch and the CompactFlash card (if installed).

Basic Port Properties


Module Properties: test_2 (Stratix 8000 1.1)
General
Connection
Module Info
Switch Configuration
Switch Status
Port Configuration
Advanced - Port Config
Unit
Port
Enable
Autonegotiate
Speed
Duplex
10 Port Base Gi1/1 0 Mbps Half Duplex
10 Port Base Gi1/2 0 Mbps Half Duplex
10 Port Base Fa1/1 0 Mbps Half Duplex
10 Port Base Fa1/2 0 Mbps Half Duplex
10 Port Base Fa1/3 0 Mbps Half Duplex
10 Port Base Fa1/4 0 Mbps Half Duplex
10 Port Base Fa1/5 0 Mbps Half Duplex
10 Port Base Fa1/6 0 Mbps Half Duplex
10 Port Base Fa1/7 0 Mbps Half Duplex
10 Port Base Fa1/8 0 Mbps Half Duplex
Expansion 1 Fa2/1 0 Mbps Half Duplex
Expansion 1 Fa2/2 100 Mbps Full Duplex
Expansion 1 Fa2/3 100 Mbps Half Duplex
Expansion 1 Fa2/4 100 Mbps Full Duplex
Refresh
Set
Status: Running
OK
Cancel
Apply
Help

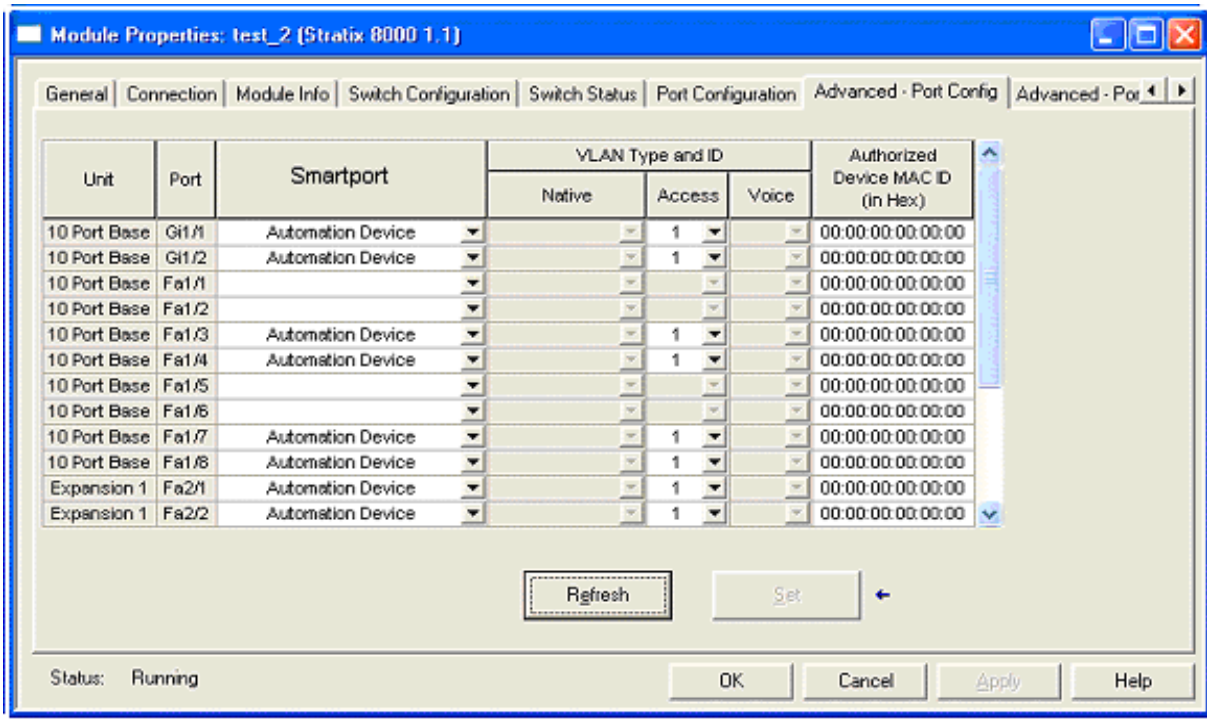
Use this tab to configure the basic switch port settings. These settings determine how data is received and sent between the switch and the attached device.

You must be online to configure the port features. Most of the information on this tab is not displayed if you are offline.

In this field	Values are	Comments
Unit	• Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).	Where the port resides.
Port	The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.	The port selected for configuration.
Enable	Check to enable the port. Clear the check box to manually disable (shut down) the port.	We recommend that you disable the port if the port is not in use and is not attached to a device. You can troubleshoot a suspected unauthorized connection by manually disabling the port.

In this field	Values are	Comments
Auto-negotiate	Check if you want the port and end-device to auto-negotiate the link speed and duplex mode. Clear the check box to manually select the desired port speed and duplex mode.	We recommend that you use the default (auto-negotiate) so that the speed and duplex settings on the switch port automatically match the setting on the connected device. Change the switch port speed and duplex if the connected device requires a specific speed and duplex. If you set the speed and duplex for the switch port, the connected device must also be configured for the exact same speed and duplex, and not set to auto-negotiate, otherwise a speed/duplex mismatch will occur. Fiber optic interfaces do not support auto-negotiation.
Speed	Gigabit (Gi): • 10 Mbps • 100 Mbps • 1 Gbps Fast Ethernet (Fa) • 10 Mbps • 100 Mbps	Choose the operating speed of the port.
Duplex	• Half-duplex – Both devices cannot send data at the same time. Half-duplex is not available when speed is set to 1 Gbps. • Full-duplex – Both devices can send data at the same time.	Choose the duplex mode of the port.

Advanced Port Properties



Use this tab to configure the Smartport roles VLAN and authorized MAC ID. You must be online to configure these port features. Most of the information on this tab is not displayed if you are offline.

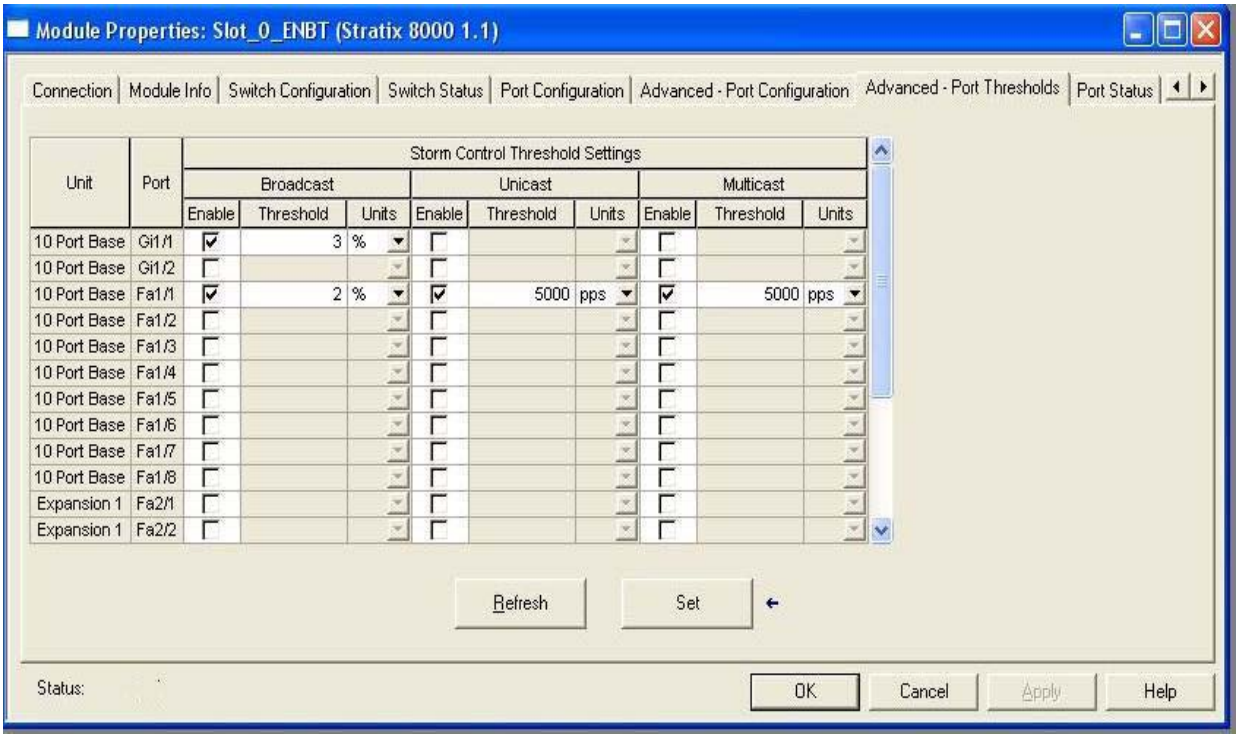
In this field	Values are	Comments
Unit	• Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).	Where the port resides.
Port	The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.	The port selected for configuration.

In this field	Values are	Comments
Smartport	Automation Device - Apply this role to ports to be connected to Ethernet/IP (Ethernet Industrial Protocol) devices. It can be used for industrial automation devices, such as logic controllers and I/O. • Port is set to Access mode. • Port security allows only one MAC ID. • Optimize queue management for CIP traffic. Automation Device with QoS - Apply this role to ports to devices that are generating 802.1Q tagged frames (not typically used). • Port is set to Trunk mode (allows 802.1Q Tagged Frames). • Portfast enabled. • Port security allows only one MAC ID. Desktop for Automation - Apply this role to ports to be connected to desktop devices, such as desktop computers, workstations, notebook computers, and other client-based hosts. • Port is set to Access mode. • Portfast enabled. • Port security allows only one MAC ID. Do not apply to ports to be connected to switches, routers, or access points. Switch for Automation - Apply this role to ports to be connected to other switches. • Port is set to Trunk mode. • Portfast enabled.	Choose the Smartport role that will be applied to the connected port. The Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and ensure security, transmission quality, and reliability to traffic from the switch ports. These configurations also prevent many problems caused by port misconfigurations. The port roles are based on the type of device that is connected to the switch port. Make sure you decide which port will be connected to which type of device before you select the Smartport.

In this field	Values are	Comments
Smartport (continued)	Router for Automation - Apply this role to routers or ports to be connected to Layer 3 switches with routing services enabled. Phone for Automation - Apply this role to ports to be connected to IP phones. A desktop device, such as a computer, can be connected to the IP phone. Both the IP phone and the connected computer would have network access through the port. • Port is set to Trunk mode. • Port security allows three MAC IDs to this port. This role prioritizes voice traffic over general data traffic to ensure clear voice reception on the IP phones. Wireless For Automation - Apply this role to ports to be connected to wireless access points. The access point can provide network access to up to 30 mobile (wireless) users. Port Mirroring - Apply this role to ports to be monitored by a network analyzer. For more information about port mirroring, see Port Mirroring on page 49. None - Apply this role to ports if you do not want a specialized Smartports role on the port. This role can be used on connections to any device, including devices in the roles described above.	Choose the Smartport role that will be applied to the connected port. The Smartport roles are recommended configurations for the ports. These configurations are referred to as port roles. They optimize the switch connections and ensure security, transmission quality, and reliability to traffic from the switch ports. These configurations also prevent many problems caused by port misconfigurations. The port roles are based on the type of device that is connected to the switch port. Make sure you decide which port will be connected to which type of device before you select the Smartport.

In this field	Values are	Comments
VLAN Type and ID	N/A	A virtual local area network (VLAN) is a logical segment of network users and resources grouped by function, team, or application. This segmentation is without regard to the physical location of the users and resources.The user can select an appropriate VLAN (native, access or voice) from a list read from the switch. Only the first 128 VLANs are displayed.
	Native	Represents the valid Native VLAN ID for ports set to the Router for Automation and Switch for Automation role. A native VLAN is for ports that can belong to a VLAN trunk (a port belonging to more than one VLAN). The Native VLAN feature is blank when Smart Port is set to any value other than Switch for Automation and Router for Automation, and in offline mode.
	Access	Represents the valid Access VLAN ID for ports set to Automation Device, Desktop for Automation, Phone for Automation for Automation, Wireless, and Automation Device with QoS role. An access VLAN is for ports that can only belong to one VLAN. The Access VLAN feature is blank when Smart Port is set to Switch for Automation and Router for Automation, and in offline mode.
	Voice	Represents the valid Voice VLAN ID for ports set to the Phone for Automation role. The voice VLAN ensures that all voice traffic has better quality of service and is not mixed with data traffic. The Voice VLAN feature is blank when Smart Port is set to any value other than Phone for Automation, and in offline mode.
Authorized Device MAC ID (in Hex)	N/A	Enter the MAC address of the device that is connected to the port. The MAC address is also known as Ethernet address, physical address, or hardware address. Each node on the network has is a unique MAC address assigned to it. The MAC ID is six hexadecimal numbers, for example 00-00-BC-22-A0-D8. You can authorize only a specific MAC address to communicate on this port. If other MAC addresses communicate on that port, they will be blocked. This feature should not be set for ports connected to other switches or routers. The Authorized Device MAC ID feature is blank in offline mode.

Port Thresholds (Storm Control)



Use this tab to set the threshold limits for broadcast, unicast, and multicast traffic for each active port. The number of packets being sent is compared against the threshold value. These limits help to prevent a single device from sending too much traffic.

In this field	Values are	Comments
Unit	• Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).	Where the port resides.
Port	The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.	The port selected for configuration.

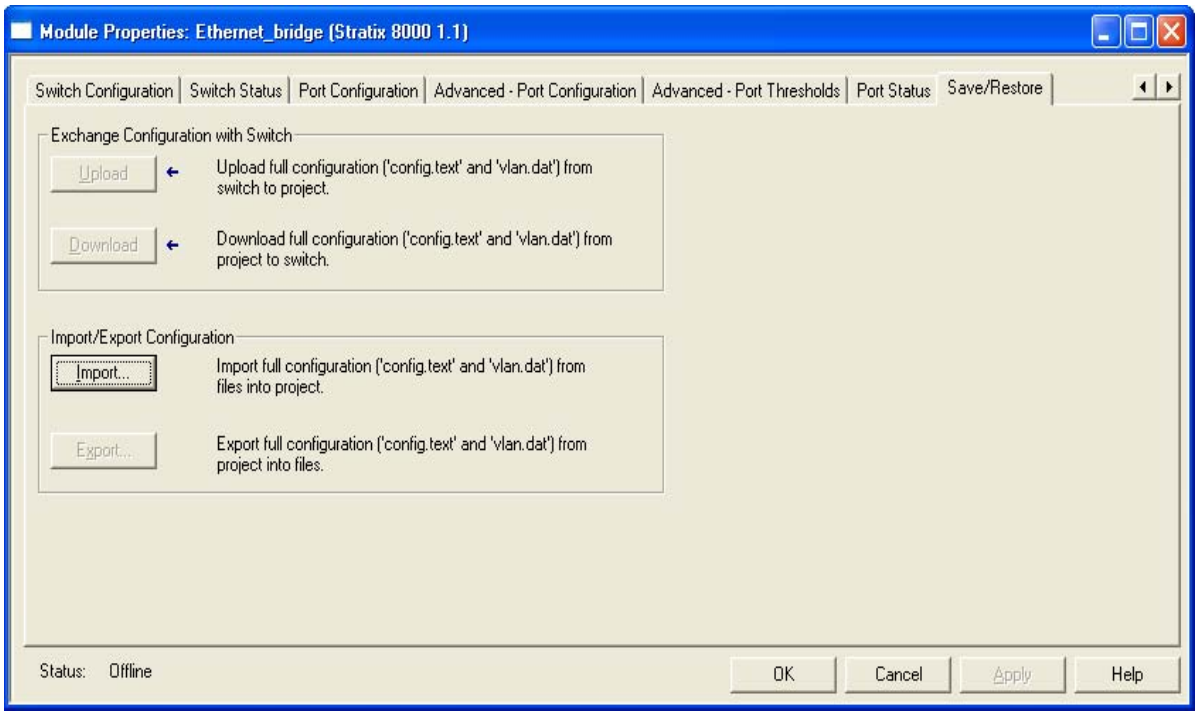
In this field	Values are	Comments
Storm Control Threshold Settings	N/A	Set the threshold values for the broadcast, unicast, and multicast traffic for each port. The number of packets being sent is compared against the threshold value. If an undesirable network event occurs and the threshold value has been exceeded, a yes value is displayed in the appropriate column in the Port Status tab and in the Traffic Exceeded on Any Port parameter in the Switch for Automation Status tab. Network traffic of the type that exceeded threshold (broadcast, unicast, or multicast) will be dropped until it falls below the falling threshold. The falling threshold is automatically set to 5% less then the entered threshold value.
Broadcast, Unicast and Multicast	Enable	Check to enable the storm control on the selected port. The respective threshold value and units are applied to the selected port when you click Set. Clear the check box to disable the storm control for the selected port. Zero (0) is applied to the threshold value and units attributes when you click Set.
	Threshold	Enter the value for the threshold after you choose the unit of measurement. If Units is set to pps or bps, enter a value between 0 and 10000000000. If Units is set to %, enter a value between 0 and 100.
	Units	Choose the unit of measurement for the threshold. The available values for each port are: • pps (packets per second). • bps (bits per second). • %.

Save and Restore Switch Configuration

Use this tab to save the switch configuration to a file for archiving, or restore a switch configuration stored locally on the computer, or within the RSLogix 5000 software project.

You must be online to save and restore configuration files. Most of the settings appear dimmed in offline mode.

You may need to enter a valid switch password to save and restore a switch configuration.



The switch configuration consists of two files:

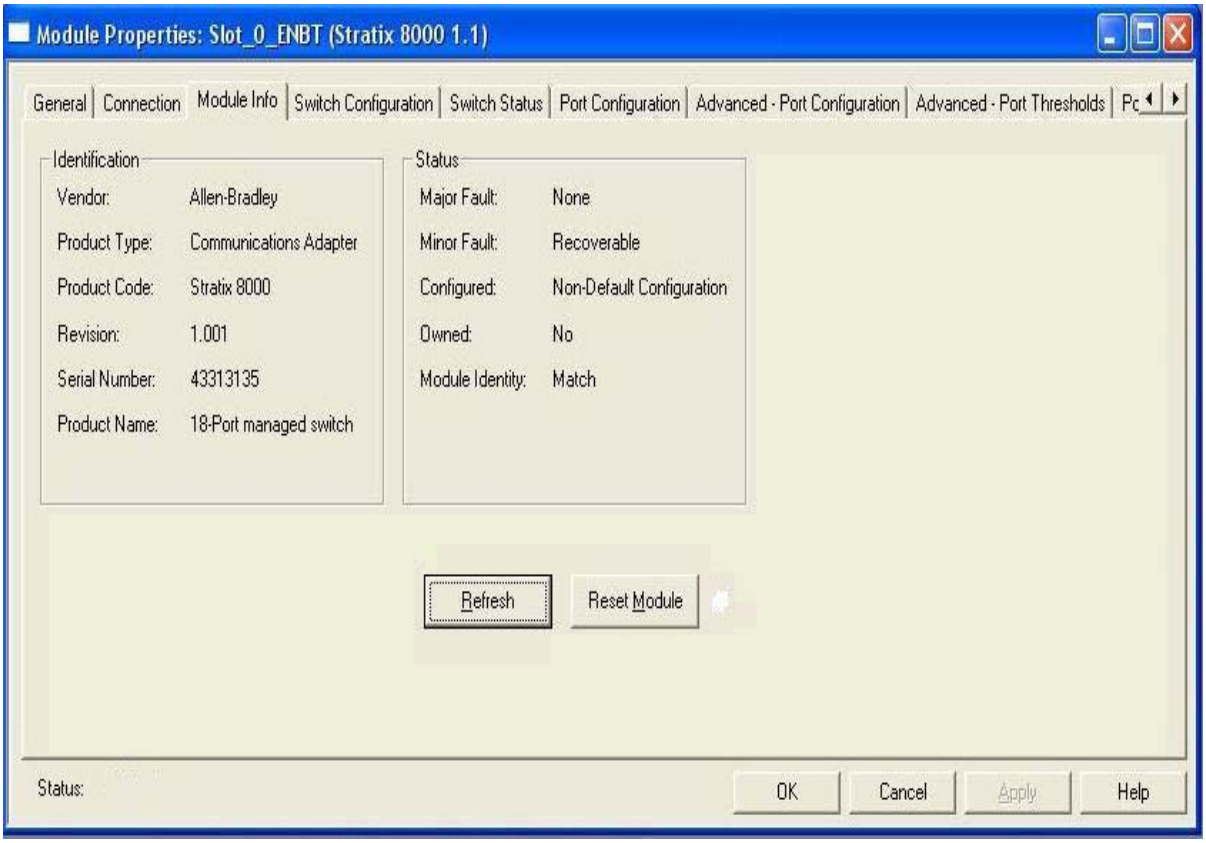
- a text file containing configuration parameters.
- a binary file containing VLAN information.

Once the switch configuration is uploaded to the RSLogix 5000 software project file, the switch configuration can be exported as computer files by using the export button.

You can import a switch configuration from the appropriate files on your computer to the project by using the Import button on the switch AOP. You can then download the configuration to the switch by using the Download button on the AOP. Refer to Save and Restore Switch Configuration on page 130 for more information on the Save and Restore feature.

Monitor and Reset the Switch

Through RSLogix 5000 software, you can monitor and reset the switch.

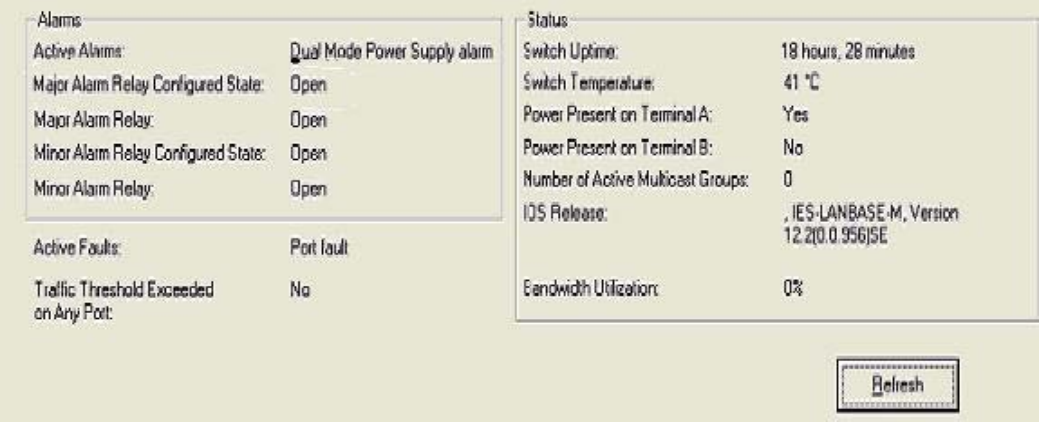


In this field	Values are	Comments
Identification	• Vendor • Product Type • Product Code • Revision • Serial Number • Product Name	Read from the switch

In this field	Values are	Comments
Status	Major/minor Fault Status • None • Recoverable • Non-recoverable Configuration • Non-default Configuration • Default Configuration Owned • Yes • No Module Identity • Match Agrees with what is specified on the General Tab. In order for the Match condition to exist, all of the following must agree: – Vendor – Product Type – Product Code – Major Revision • Mismatch Does not agree with what is specified on the General tab. Refresh Click to refresh the tab with new data from the module. Reset Module Click to perform a switch reset (power cycle) with the current configuration file. The Password Confirmation dialog box may appear. **Attention:** Resetting a module causes all connections to or through the module to be closed, and this may result in loss of control.	Indicates whether there is an I/O connection. This field does not take into account the Electronic Keying or Minor Revision selections for the switch that were specified on the General tab.

Switch Status

Through RSLogix 5000 software, you can monitor switch status. Use this tab to monitor the switch and port conditions to quickly see if a fault or error condition exists. This tab also shows the overall health of the switch (temperature and power).

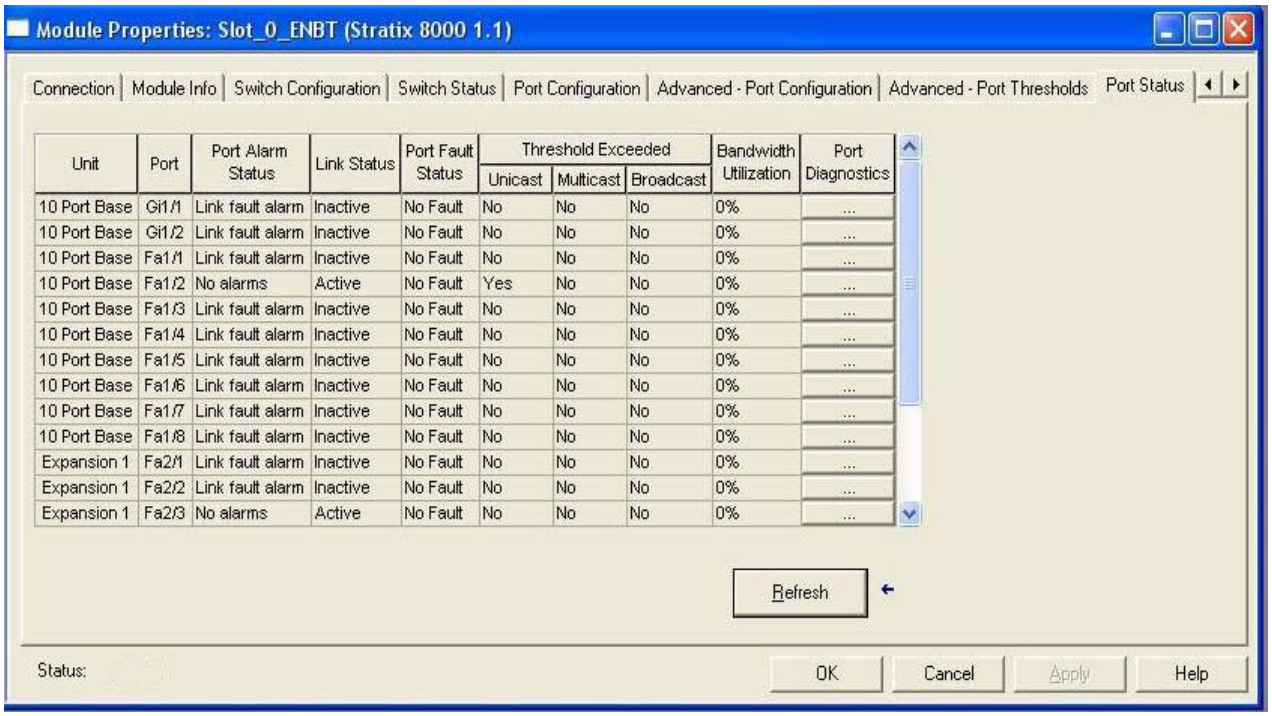


In this field	Values are	Comments
Alarms	• Active Alarms	Displays the active switch and port alarms. The available values are: • None. • Port alarm. • Dual Mode Power Supply alarm. • Primary Temperature alarm.
	• Major Alarm Relay Configured State	Displays whether the major alarm relay is configured.
	• Major Alarm Relay	Displays whether the major alarm relay is on or off.
	• Minor Alarm Relay Configured State	Displays whether the minor alarm relay is configured.
	• Minor Alarm Relay	Displays whether the minor alarm relay is on or off.
Active Faults		Displays the active switch and port faults. The available values are: • None. • Port fault. • Hardware fault. If the port and hardware faults are active, the Hardware fault will be displayed.

In this field	Values are	Comments
Traffic Threshold Exceeded on Any Port		Displays a yes or no value indicating whether the current unicast, multicast, and broadcast thresholds have been exceeded on any port. To view the status of the active ports, click the Port Status tab. To view the threshold values, click the Advanced - Port Threshold tab.
Status		These features display the status of the switch.
	Switch Uptime	Displays the days, hours, and minutes that the switch has been functioning since the last reboot.
	Switch Temperature	Displays the current internal temperature (in degree Celsius) of the switch.
	Power Present on Terminal A	Displays a yes or no value indicating whether power is present on Terminal A.
	Power Present on Terminal B	Displays a yes or no value indicating whether power is present on Terminal B.
	Number of Active Multicast Groups	Displays the number of active multicast groups.
	IOS Release	Displays the current version of the switch operating system.
	Bandwidth Utilization	Displays the total percentage of the switch bandwidth being used.

Port Status

Through RSLogix 5000 software, you can monitor port status.

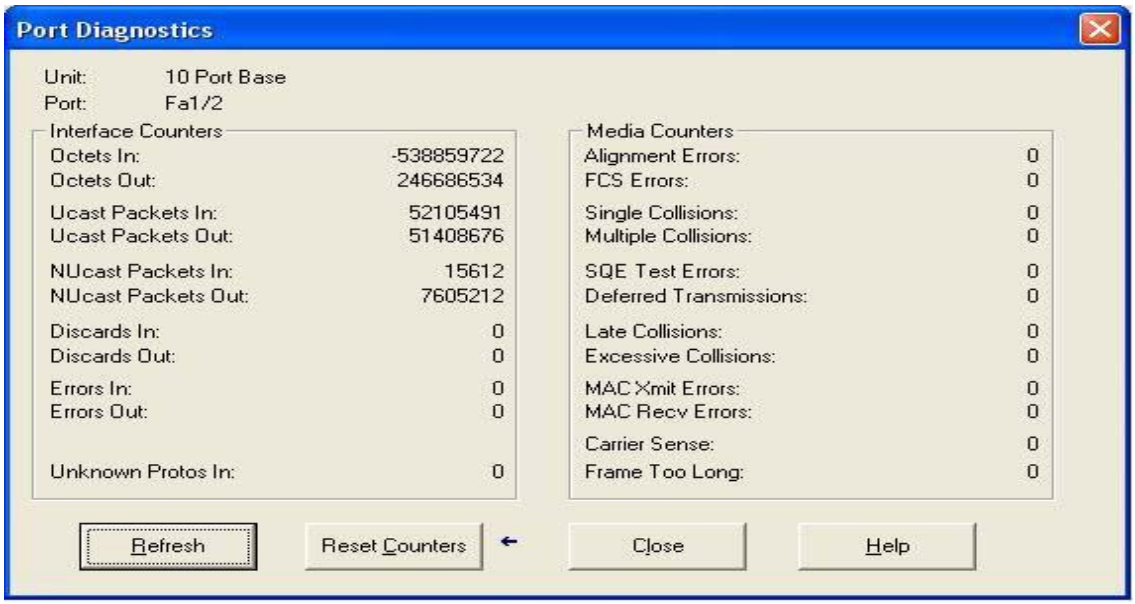

Module Properties: Slot_0_ENBT (Stratix 8000 1.1)
Connection
Module Info
Switch Configuration
Switch Status
Port Configuration
Advanced - Port Configuration
Advanced - Port Thresholds
Port Status
Unit
Port
Port Alarm Status
Link Status
Port Fault Status
Threshold Exceeded
Unicast
Multicast
Broadcast
Bandwidth Utilization
Port Diagnostics
10 Port Base Gi1/1 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Gi1/2 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/1 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/2 No alarms Active No Fault Yes No No 0%
10 Port Base Fa1/3 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/4 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/5 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/6 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/7 Link fault alarm Inactive No Fault No No No 0%
10 Port Base Fa1/8 Link fault alarm Inactive No Fault No No No 0%
Expansion 1 Fa2/1 Link fault alarm Inactive No Fault No No No 0%
Expansion 1 Fa2/2 Link fault alarm Inactive No Fault No No No 0%
Expansion 1 Fa2/3 No alarms Active No Fault No No No 0%
Refresh
Status:
OK
Cancel
Apply
Help

In this field	Values are	Comments
Unit	• Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).	Where the port resides.
Port	The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.	The port selected for configuration.
Port Alarm Status	• Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms	Displays the current status of the port alarm.
Link Status	• Active • Inactive	Displays link activity status.

In this field	Values are	Comments
Port Fault Status	• Error-disable event • SFP error-disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault	Displays the current status of the port fault.
Threshold Exceeded	• Unicast Displays a yes or no value indicating whether the current unicast traffic has exceeded the threshold value. • Multicast Displays a yes or no value indicating whether the current multicast traffic has exceeded the threshold value. • Broadcast Displays a yes or no value indicating whether the current broadcast traffic has exceeded the threshold value.	If the threshold value (set in Advanced->Port Threshold tab) has been exceeded, a yes value displays in the appropriate column. If the threshold value has not been exceeded, a no value displays in the appropriate column.
Bandwidth Utilization	N/A	Displays the percentage of the bandwidth being used. Note whether the percentage of usage is what you expect during the given time of network activity. If usage is higher than you expected, a problem might exist.
Port Diagnostics	N/A	Click to display the Port Diagnostic dialog box for the corresponding port. The Port Diagnostic screen provides you information to diagnose a network performance problem.

Use the Port Diagnostics dialog box to view the status of the link performance. You can:

- view octet and packet counters.
- view collisions on the link.
- view errors on the link.
- reset and clear all status counters.



In this field	Values are	Comments
Unit	• Base (for example, 1783-MS10T). • Expansion module (for example, 1783-MX08T).	Where the port resides.
Port	The port number includes the port type (Fa for Fast Ethernet and Gi for Gigabit Ethernet), the base or expansion module number (1, 2, or 3), and the specific port number. For example: • Gi1/1 is Gigabit Ethernet port 1 on the base. • Fa2/1 is Fast Ethernet port 1 on the first expansion module.	The port selected for configuration.

In this field	Values are	Comments
Interface Counters	• Octets In – the number of octets received by the port. • Octets Out – the number of octets sent by the port. • Ucast Packets In – the number of unicast packets received by the port. • Ucast Packets Out – the number of unicast packets sent by the port. • NUcast packets In – the number of multicast packets received by the port. • NUcast packets Out – the number of multicast packets sent by the port. • Discards In – the number of inbound packets that have been discarded. • Discards Out – the number of outbound packets that have been discarded. • Errors In – the number of inbound packets that contain errors. • Errors Out – the number of outbound packets that contain errors. • Unknown Protos (Protocols) In – the number of inbound packets with unknown protocols.	Lets you to view status of octets received and sent, and packets received and sent.

In this field	Values are	Comments
Media Counters	Collisions • Single – the number of single collisions. • Multiple – the number of multiple collisions. • Late – the number of late collisions. • Excessive – the number of frames for which transmission fails due to excessive collisions.	These counters allow you to view the number of collisions on a link.
	Errors • Alignment – the number of frames received that are not an integral number of octets in length. • FCS (Frame Check Sequence) – the number of frames received that do not pass the FCS check. • SQE Test Errors – the number of times that the SQE TEST ERROR message is generated. • Deferred Transmissions – count of transmissions deferred by busy network. • MAC Xmit Errors – the number of frames that failed to transmit due to an internal MAC sublayer transmit error. • MAC Recv Errors – the number of frames that failed to be received due to an internal MAC sublayer receive error. • Carrier Sense – the number of times the carrier sense condition was lost or never asserted when attempting to transmit a frame. • Frame Too Long – the number of frames received that exceed the maximum permitted frame size.	These counters allow you to view errors.

Notes:

Troubleshoot the Switch

Introduction

This chapter helps you resolve issues related to Stratix 8000 and Stratix 8300 switches, as well as perform common functions such as resetting the switch.

To resolve hardware issues related to connectivity between the switch and other devices, see the Stratix 8000 and Stratix 8300 Ethernet Managed Switches Installation Instructions, publication 1783-IN005.

Topic	Page
Run a Diagnostic Test	141
IP Address Issues	143
Device Manager Issues	144
Switch Performance	144
Access Direct Managed Mode	146
Restart or Reset the Switch	147
Recover the Switch Firmware and Restore Factory Defaults	149
Troubleshoot a Firmware Upgrade	150

Run a Diagnostic Test

When the switch detects an issue, the Status field on the front panel view in the Device Manager Web interface lists the detected issue. From the Diagnostic Test dialog box, you can run switch and link diagnostic tests to help you resolve issues.

- The switch diagnostic test detects system and port issues on the switch. For example:
  - Power-on self-test (POST) error.
  - Port-to-Smartports configuration mismatch.
  - Duplex mode mismatch.

- The link diagnostic test on a specific port detects speed mismatch and cable-related issues on the port or the circuit, such as:
  - Unconnected cable.
  - Cable too short or too long.
  - Faulty cable.

TIP The link test is run on a port that is not in a link-up state because it can interrupt traffic between the switch port and its connected device. Run the link test only on a port that has a suspected issue. Before running the link test, use the Front Panel view, the Port Status, and the Port Statistics dialog boxes to determine the details of the issue.

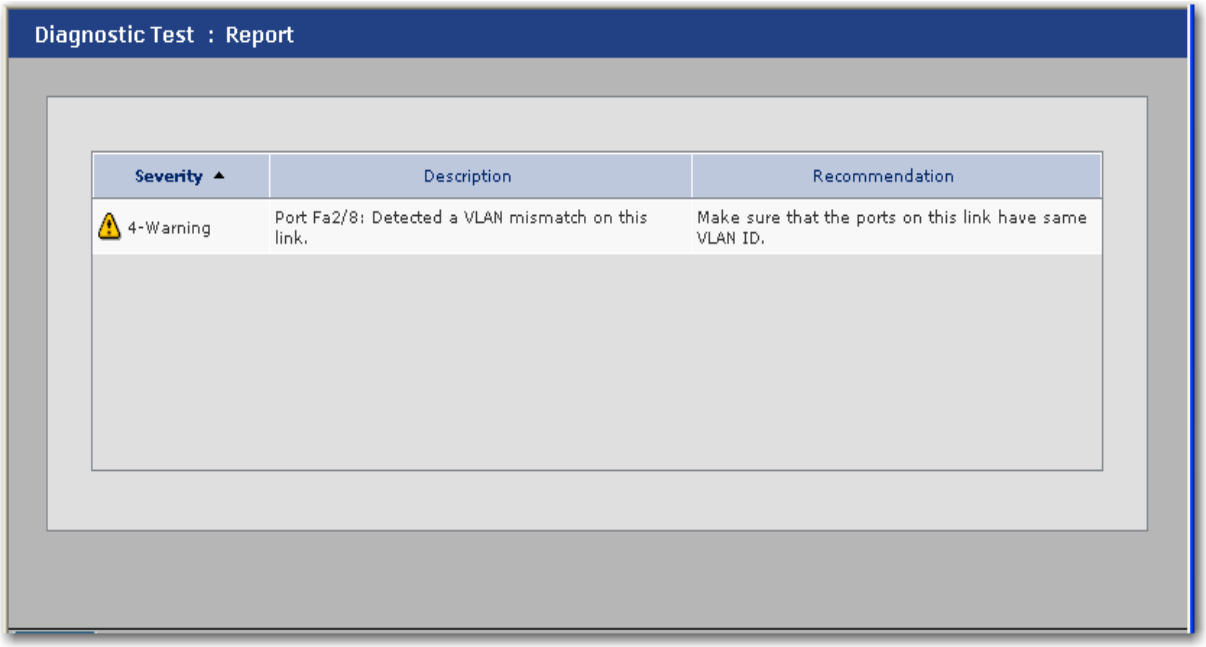
TIP Use the diagnostics report with the Alert Log. The log includes the last time at which the issues were detected by the switch.

To display the Diagnostic Test dialog box, choose Maintenance >Diagnostic Test from the Device Manager Web interface menu.

You can also display the Diagnostic Test dialog box by clicking Get Details in the Status field, which is displayed under the Front Panel view.

After either or both tests run, the dialog box displays a report, shown in the following figure, that lists issues detected by the switch.

The report also includes severity levels and recommended actions to help you solve the issues.


Diagnostic Test : Report
Severity
Description
Recommendation
4-Warning
Port Fa2/8: Detected a VLAN mismatch on this link.
Make sure that the ports on this link have same VLAN ID.

The diagnostics report includes this information..

Field	Description
Severity Level	A single-digit code (0…5) that reflects the severity of the issue. The lower the number, the more serious the condition and the need to take action. Emergency (0)—The switch is unusable. Alert (1)—The switch requires immediate action. Critical (2)—The switch has a critical condition. Error (3)—The switch has an error condition. Warning (4)—The switch has a warning condition. Notifications (5)—The switch is operating normally but has a significant condition.
Description	The description of the issue, including the port on which the issue was detected.
Recommendation	The recommended actions you should take to solve the issue.

IP Address Issues

Following are some basic troubleshooting tips for issues related to the switch IP address.

Issue	Resolution
IP address is not received from DHCP server	If the switch does not receive an IP address from an upstream device operating as a DHCP server, make sure that the upstream device is operating as a DHCP server and again follow the procedures to set up the switch in Chapter 1, Getting Started.
Switch has wrong IP address	If the switch is installed in your network but you cannot access the switch because it has the wrong IP address, assign a new switch IP address. Refer to Access Direct Managed Mode on page 146 to assign the IP address, and then update the switch IP address on the Device Manager Express Setup window.

Device Manager Issues

Following are some basic troubleshooting for issues related to displaying the Device Manager Web interface.

Issue	Resolution
Device Manager Web interface does not display	If you cannot display the Device Manager Web interface from your computer or laptop, make sure that you entered the correct switch IP address in the browser. If you entered the correct switch IP address in the browser, make sure that the switch and your computer or laptop are in the same network or subnetwork. For example: • If your switch IP address is 172.20.20.85 and your computer or laptop IP address is 172.20.20.84, both devices are in the same network. • If your switch IP address is 172.20.20.85 and your computer or laptop IP address is 10.0.0.2, the devices are in different networks and cannot directly communicate without a router. You must either change the switch IP address or change the computer or laptop IP address. • If the issue persists, follow the procedure in the Access Direct Managed Mode section on page 146, and then update the switch network settings on the device manager Express Setup window. • If the issue still persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 149.
Device Manager Web interface is not operating properly	If the Device Manager Web interface does not operate properly (for instance, the device manager is not responding), follow the procedure in the Access Direct Managed Mode section on page 146, and then update the switch network settings on the Device Manager Web interface Express Setup window. If the issue persists, follow the procedure in the Recover the Switch Firmware and Restore Factory Defaults section on page 149.
Device Manager Web interface is not accessible through the network	If you cannot access the device manager remotely from a Web browser, follow the procedure in the Access Direct Managed Mode section on page 146.

Switch Performance

Following are some basic troubleshooting for issues related to switch performance.

Issue	Resolution
Speed, Duplex, and Autonegotiation	If the port statistics show a large amount of alignment errors, frame check sequence (FCS), or late-collisions errors, this might indicate a speed or duplex mismatch. A common issue with speed and duplex occurs when the duplex settings are mismatched between two switches, between a switch and a router, or between the switch and a workstation or server. This can happen when manually setting the speed and duplex or from autonegotiation issues between the two devices. A mismatch occurs under these circumstances: • A manually set speed or duplex parameter is different from the manually set speed or duplex parameter on the connected port. • A port is set to autonegotiate, and the connected port is set to full-duplex with no autonegotiation. To maximize switch performance and ensure a link, follow one of these guidelines when changing the settings for duplex and speed: • Let both ports autonegotiate both speed and duplex. • Manually set the same speed and duplex parameters for the ports on both ends of the connection to the same values. • If a remote device does not autonegotiate, configure the duplex settings on the two ports to the same values. The speed parameter can adjust itself even if the connected port does not autonegotiate.
Autonegotiation and Network Interface Cards (NICs)	Issues sometimes occur between the switch and third-party network interface cards (NICs). By default, the switch ports and interfaces are set to autonegotiate. It is common for devices like laptops or other devices to be set to autonegotiate as well, yet sometimes autonegotiation issues occur. To troubleshoot autonegotiation issues, try manually setting both sides of the connection. If this does not solve the issue, there could be an issue with the firmware or software on your NIC. You can resolve this by upgrading the NIC driver to the latest version available from the manufacturer.
Cabling distance	If the port statistics show excessive FCS, late-collision, or alignment errors, verify that the cable distance from the switch to the connected device meets the recommended guidelines.

Access Direct Managed Mode

You can display the Device Manager Web interface and manage the switch through a physical connection between one of the switch ports and your computer or laptop. This type of management connection is referred to as the Direct Managed mode. This mode is typically used to connect to the switch by using the Device Manager Web interface when the IP address of the switch is unknown.

Before you can access Direct Managed mode, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

To access the Direct Managed mode, follow these steps.

1. Press the Express Setup button until the Setup status indicator blinks green and the status indicator of an available switch downlink port blinks green.

   The port with a blinking green status indicator is designated as the direct managed mode port. This port is determined by the following:

   - If all downlink ports are not connected to devices or if multiple downlink ports are connected to devices, the first available downlink port is selected as the direct managed mode port.
   - If only one downlink port is connected to a device, that port is selected as the direct managed mode port.

   If there is no available switch downlink port to which to connect your computer or laptop, disconnect a device from one of the switch downlink ports, and then press the Setup button again until the Setup status indicator and the port status indicator blink green.

2. Use a Category 5 Ethernet cable to connect your computer or laptop to the switch port with the blinking port status indicator.

3. Wait until the port status indicators on the switch and your computer or laptop are solid green.

   The solid green port status indicators means a successful connection between the two devices.

4. Start a Web browser on your computer or laptop.

   A password prompt, followed by the Device Manager Web interface page appears.

If the Device Manager Web interface does not appear, make sure that any pop-up blockers or proxy settings in your browser software are disabled and that any wireless clients running on your computer or laptop are disabled.

If the Device Manager Web interface still does not appear, enter a URL in your browser, such as http://www.rockwellautomation.com. The browser should redirect to the Device Manager Web interface.

Restart or Reset the Switch

If you cannot solve an issue by reconfiguring a feature, either restarting or resetting the switch might solve the issue or help you to eliminate probable causes. If the issue exists after you reset the switch to its default settings, it is unlikely that the switch is causing the issue.

Option	Description
Restart	This option restarts the switch without turning off power. The switch retains its saved configuration settings during the restart process. However, the Device Manager Web interface is unavailable during the process. When the process completes, the switch displays the Device Manager Web interface. **Important:** Restarting the switch interrupts connectivity of your devices to the network.
Reset the Switch to Factory Defaults	This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch. **Attention:** Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to the factory default settings. The same software image is retained. You need to reconfigure the basic switch settings. Refer to Initialize the Switch with Express Setup on page 17. **Attention:** Resetting the switch interrupts connectivity of your devices to the network.

IMPORTANT Restarting or resetting the switch interrupts connectivity of your devices to the network.

Restart the Switch from the Device Manager Web Interface

From the Device Manager Web interface, on the Restart/Reset dialog box, click Restart the Switch.

This option restarts the switch without turning off power. The Device Manager Web interface is unavailable during the restart process. When the process completes, the switch displays the Device Manager Web interface.

If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode section on page 146 to access Direct Managed mode.

Restart the Switch from RSLogix 5000 Programming Software

Using RSLogix 5000 software, do the following.

1. Click the Module Info tab.
2. Click Reset Module.

   A password prompt appears.
3. Enter your password and click Enter.

Reset the Switch to Factory Defaults

ATTENTION

Resetting the switch deletes all customized switch settings, including the IP address, and returns the switch to its factory default. The same software image is retained. To manage the switch or to display the device manager, you need to reconfigure the basic switch settings (as described in Chapter 3, Manage the Switch via the Device Manager Web Interface) and use the new IP address.

IMPORTANT

Restarting the switch interrupts connectivity of your devices to the network.

From the Device Manager Web interface, do the following.

1. Access the Device Manager Web interface Restart/Reset dialog box.
2. Click Reset the Switch.

This option resets the switch, deletes the current configuration settings, returns to the factory default settings, and then restarts the switch.

If you do not know the switch IP address, follow the procedure in the Access Direct Managed Mode section on page 146 to access Direct Managed mode. Then go back to step 1, above.

Recover the Switch Firmware and Restore Factory Defaults

Before you can recover switch firmware, you must make sure of the following:

- You must have physical access to the switch.
- Make sure that at least one switch port is enabled and is not connected to a device.

You might need to recover the switch firmware if the image is corrupted. A symptom of corrupted firmware is the switch continuously trying to restart.

Other reasons to recover the switch firmware are if you deleted the image due to a failed firmware upgrade and if you have forgotten the switch password.

Recovering the switch firmware involves deleting all switch configuration settings and returning the switch to its factory default settings. To return the switch to its factory default settings, follow these steps.

1. Remove power from the switch.
2. Reapply power to the switch.
3. While the switch is powering up, press and hold the Express Setup button.
4. When the EIP Mod, EIP Net and Setup status indictors turn red, release the Express Setup button.

   The switch continues powering up in its factory default state.
5. Set up the switch, as described in Chapter 1, Getting Started .
6. Refer to Troubleshoot a Firmware Upgrade on page 150 and follow the procedure to upgrade the firmware.

Troubleshoot a Firmware Upgrade

If you attempted to upgrade the switch firmware but received a message that the upgrade failed, make sure that you still have access to the switch. If you still have switch access, follow these steps.

1. Make sure that you downloaded the correct tar file from http://www.rockwellautomation.com.

2. If you downloaded the correct tar file, refresh your Device Manager Web interface browser session to make sure that there is connectivity between the switch and your computer or laptop or network drive.
   - If you have connectivity to the switch and the Device Manager Web interface, retry the upgrade.
   - If you do not have connectivity to the switch and the Device Manager Web interface, refer to Recover the Switch Firmware and Restore Factory Defaults on page 149.

I/O Data Types

Pre-defined RSLogix 5000 tags for Input and Output data types have a structure corresponding to the switch (module) selected when it was added to the I/O tree. Its members are named in accordance with the port names.For example, if a user selects the 18-port switch, the 18 port names corresponding to that module are visible. The other member names (19...26) are hidden.

You can disable a switch port by setting the corresponding bit in the output tag. The output bits will be applied every time the switch receives the output data from the controller when the controller is in Run mode. When the controller is in Program mode, the output bits are not applied.

The port is enabled if the corresponding output bit is 0. If you enable or disable a port by using the Device Manager Web interface or the CLI, the port setting may be overridden by the output bits the next time they are applied. The output bits will always take precedence, regardless of whether the Device Manager Web interface or CLI was used to enable or disable the port.

The following tables show input and output data types for all 26 ports of the switch, as well as port assignments for data types.

Input Tags

Tag Name	Type	Description
I:Fault	DINT	If there is s communication fault between the controller and the switch all 32 bits in the module fault word are set to 1
I:AnyPortConnected	BOOL	Indicates that at least one port has a link status or active
I:PortGi1_1Connected	BOOL	Indicates that a particular port has link status active 0 = Link not active 1 = Link active
I:PortGi1_2Connected	BOOL	
I:PortFa1_1Connected	BOOL	
I:PortFa1_2Connected	BOOL	
I:PortFa1_3Connected	BOOL	
I:PortFa1_4Connected	BOOL	
I:PortFa1_5Connected	BOOL	
I:PortFa1_6Connected	BOOL	

Input Tags

Tag Name	Type	Description
I:PortFa1_7Connected	BOOL	Indicates that a particular port has link status active 0 = Link not active 1 = Link active
I:PortFa1_8Connected	BOOL	
I:PortFa2_1Connected	BOOL	
I:PortFa2_2Connected	BOOL	
I:PortFa2_3Connected	BOOL	
I:PortFa2_4Connected	BOOL	
I:PortFa2_5Connected	BOOL	
I:PortFa2_6Connected	BOOL	
I:PortFa2_7Connected	BOOL	
I:PortFa2_8Connected	BOOL	
I:PortFa3_1Connected	BOOL	
I:PortFa3_2Connected	BOOL	
I:PortFa3_3Connected	BOOL	
I:PortFa3_4Connected	BOOL	
I:PortFa3_5Connected	BOOL	
I:PortFa3_6Connected	BOOL	
I:PortFa3_7Connected	BOOL	
I:PortFa3_8Connected	BOOL	
I:AnyPortUnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on any port
I:PortGi1_1UnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on a particular port 0 = No mismatch 1 = Mismatch
I:PortGi1_2UnauthorizedDevice	BOOL	
I:PortFa1_1UnauthorizedDevice	BOOL	
I:PortFa1_2UnauthorizedDevice	BOOL	
I:PortFa1_3UnauthorizedDevice	BOOL	
I:PortFa1_4UnauthorizedDevice	BOOL	
I:PortFa1_5UnauthorizedDevice	BOOL	
I:PortFa1_6UnauthorizedDevice	BOOL	
I:PortFa1_7UnauthorizedDevice	BOOL	
I:PortFa1_8UnauthorizedDevice	BOOL	
I:PortFa2_1UnauthorizedDevice	BOOL	
I:PortFa2_2UnauthorizedDevice	BOOL	
I:PortFa2_3UnauthorizedDevice	BOOL	
I:PortFa2_4UnauthorizedDevice	BOOL	
I:PortFa2_5UnauthorizedDevice	BOOL	
I:PortFa2_6UnauthorizedDevice	BOOL	
I:PortFa2_7UnauthorizedDevice	BOOL	
I:PortFa2_8UnauthorizedDevice	BOOL	
I:PortFa3_1UnauthorizedDevice	BOOL	

Input Tags

Tag Name	Type	Description
I:PortFa3_2UnauthorizedDevice	BOOL	Indicates that an unauthorized MAC ID has attempted to communicate on a particular port 0 = No mismatch 1 = Mismatch
I:PortFa3_3UnauthorizedDevice	BOOL	
I:PortFa3_4UnauthorizedDevice	BOOL	
I:PortFa3_5UnauthorizedDevice	BOOL	
I:PortFa3_6UnauthorizedDevice	BOOL	
I:PortFa3_7UnauthorizedDevice	BOOL	
I:PortFa3_8UnauthorizedDevice	BOOL	
I:AnyPortThreshold	BOOL	Indicates that unicast, multicast or broadcast threshold limit has been exceeded on any port
I:PortGi1_1Threshold	BOOL	Indicates that unicast, multicast or broadcast threshold limit has been exceeded on a particular port 0 = OK 1 = Threshold exceeded
I:PortGi1_2Threshold	BOOL	
I:PortFa1_1Threshold	BOOL	
I:PortFa1_2Threshold	BOOL	
I:PortFa1_3Threshold	BOOL	
I:PortFa1_4Threshold	BOOL	
I:PortFa1_5Threshold	BOOL	
I:PortFa1_6Threshold	BOOL	
I:PortFa1_7Threshold	BOOL	
I:PortFa1_8Threshold	BOOL	
I:PortFa2_1Threshold	BOOL	
I:PortFa2_2Threshold	BOOL	
I:PortFa2_3Threshold	BOOL	
I:PortFa2_4Threshold	BOOL	
I:PortFa2_5Threshold	BOOL	
I:PortFa2_6Threshold	BOOL	
I:PortFa2_7Threshold	BOOL	
I:PortFa2_8Threshold	BOOL	
I:PortFa3_1Threshold	BOOL	
I:PortFa3_2Threshold	BOOL	
I:PortFa3_3Threshold	BOOL	
I:PortFa3_4Threshold	BOOL	
I:PortFa3_5Threshold	BOOL	
I:PortFa3_6Threshold	BOOL	
I:PortFa3_7Threshold	BOOL	
I:PortFa3_8Threshold	BOOL	
I:AllPortsUtilization	SINT	The sum of the percentage of the bandwidth utilized of all ports on the switch
I:PortGi1_1Utilization;	SINT	The percentage of the bandwidth utilized on a particular port
I:PortGi1_2Utilization;	SINT	
I:PortFa1_1Utilization;	SINT	

Input Tags

Tag Name	Type	Description
I:PortFa1_2Utilization;	SINT	The percentage of the bandwidth utilized on a particular port
I:PortFa1_3Utilization;	SINT	
I:PortFa1_4Utilization;	SINT	
I:PortFa1_5Utilization;	SINT	
I:PortFa1_6Utilization;	SINT	
I:PortFa1_7Utilization;	SINT	
I:PortFa1_8Utilization;	SINT	
I:PortFa2_1Utilization;	SINT	
I:PortFa2_2Utilization;	SINT	
I:PortFa2_3Utilization;	SINT	
I:PortFa2_4Utilization;	SINT	
I:PortFa2_5Utilization;	SINT	
I:PortFa2_6Utilization;	SINT	
I:PortFa2_7Utilization;	SINT	
I:PortFa2_8Utilization;	SINT	
I:PortFa3_1Utilization;	SINT	
I:PortFa3_2Utilization;	SINT	
I:PortFa3_3Utilization;	SINT	
I:PortFa3_4Utilization;	SINT	
I:PortFa3_5Utilization;	SINT	
I:PortFa3_6Utilization;	SINT	
I:PortFa3_7Utilization;	SINT	
I:PortFa3_8Utilization;	SINT	
I:MajorAlarmRelay	BOOL	Indicates whether the major alarm relay is on or off 0 = Contact open (off) 1 = Contact closed (on)
I:MinorAlarmRelay	BOOL	Indicates whether the minor alarm relay is on or off 0 = Contact open (off) 1 = Contact closed (on)
I:MulticastGroupsActive	DINT	The number of active multicast groups across all ports

Output Tags

Tag Name	Type	Description
O:AllPortsDisable	BOOL	Setting this bit disables all ports on the switch 0 = Enable 1 = Disable
O:PortGi1_1Disable	BOOL	Setting a particular bit disables that particular port 0 = Enable 1 = Disable
O:PortGi1_2Disable	BOOL	
O:PortFa1_1Disable	BOOL	
O:PortFa1_2Disable	BOOL	
O:PortFa1_3Disable	BOOL	
O:PortFa1_4Disable	BOOL	
O:PortFa1_5Disable	BOOL	
O:PortFa1_6Disable	BOOL	
O:PortFa1_7Disable	BOOL	
O:PortFa1_8Disable	BOOL	
O:PortFa2_1Disable	BOOL	
O:PortFa2_2Disable	BOOL	
O:PortFa2_3Disable	BOOL	
O:PortFa2_4Disable	BOOL	
O:PortFa2_5Disable	BOOL	
O:PortFa2_6Disable	BOOL	
O:PortFa2_7Disable	BOOL	
O:PortFa2_8Disable	BOOL	
O:PortFa3_1Disable	BOOL	
O:PortFa3_2Disable	BOOL	
O:PortFa3_3Disable	BOOL	
O:PortFa3_4Disable	BOOL	
O:PortFa3_5Disable	BOOL	
O:PortFa3_6Disable	BOOL	
O:PortFa3_7Disable	BOOL	
O:PortFa3_8Disable	BOOL	

Notes:

Port Assignments for CIP Data

This table identifies the instance numbers of the Ethernet link object associated with each port on the switch. Instance 0 does not apply to all the ports as it does for bit maps.

The bit numbers identify each port when they are contained n a structure of all the ports, for example, in the output assembly. Bit 0 refers to any or all ports.

Port Assignments for CIP Data

Instance/Bit	6-port Managed Ethernet Switch	14-port Managed Ethernet Switch	22-port Managed Ethernet Switch	10-port Managed Ethernet Switch	18-port Managed Ethernet Switch	26-port Managed Ethernet Switch
Bit 0	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports	Any/All ports
Instance/Bit 1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1	Gi1/1
Instance/Bit 2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2	Gi1/2
Instance/Bit 3	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
Instance/Bit 4	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
Instance/Bit 5	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
Instance/Bit 6	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
Instance/Bit 7				Fa1/5	Fa1/5	Fa1/5
Instance/Bit 8				Fa1/6	Fa1/6	Fa1/6
Instance/Bit 9				Fa1/7	Fa1/7	Fa1/7
Instance/Bit 10				Fa1/8	Fa1/8	Fa1/8
Instance/Bit 11		Fa2/1	Fa2/1		Fa2/1	Fa2/1
Instance/Bit 12		Fa2/2	Fa2/2		Fa2/2	Fa2/2
Instance/Bit 13		Fa2/3	Fa2/3		Fa2/3	Fa2/3
Instance/Bit 14		Fa2/4	Fa2/4		Fa2/4	Fa2/4
Instance/Bit 15		Fa2/5	Fa2/5		Fa2/5	Fa2/5
Instance/Bit 16		Fa2/6	Fa2/6		Fa2/6	Fa2/6
Instance/Bit 17		Fa2/7	Fa2/7		Fa2/7	Fa2/7
Instance/Bit 18		Fa2/8	Fa2/8		Fa2/8	Fa2/8
Instance/Bit 19			Fa3/1			Fa3/1
Instance/Bit 20			Fa3/2			Fa3/2
Instance/Bit 21			Fa3/3			Fa3/3
Instance/Bit 22			Fa3/4			Fa3/4
Instance/Bit 23			Fa3/5			Fa3/5

Port Assignments for CIP Data

Instance/Bit	6-port Managed Ethernet Switch	14-port Managed Ethernet Switch	22-port Managed Ethernet Switch	10-port Managed Ethernet Switch	18-port Managed Ethernet Switch	26-port Managed Ethernet Switch
Instance/Bit 24			Fa3/6			Fa3/6
Instance/Bit 25			Fa3/7			Fa3/7
Instance/Bit 26			Fa3/8			Fa3/8

Cables and Connectors

10/100 and 10/100/1000 Ports

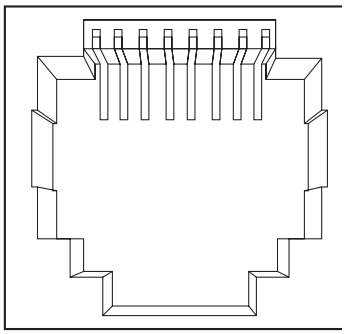
The 10/100 and 10/100/1000 Ethernet ports on switches use standard RJ45 connectors and Ethernet pinouts with internal crossovers.

TIP The auto-MDIX feature is enabled by default.

The following figure shows the connector pinouts.

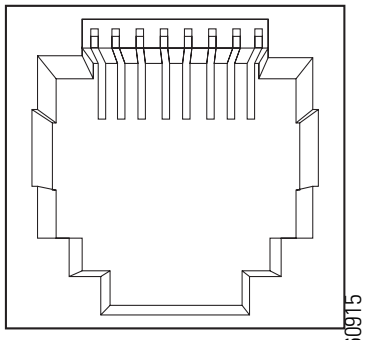
10/100 Connector Pinouts

Pin	Label
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC



10/100/1000 Connector Pinouts

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



Connect to 10BASE-T- and 100BASE-TX-Compatible Devices

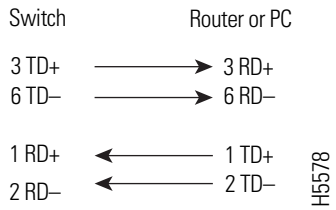
When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as servers, workstations, and routers, you can use a two or four twisted-pair, straight-through cable wired for 10BASE-T and 100BASE-TX.

To identify a crossover cable, compare the two modular ends of the cable. Hold the cable ends side-by-side, with the tab at the back. The wire connected to the pin on the outside of the left plug should be a different color from the wire connected to the pin on the inside of the right plug.

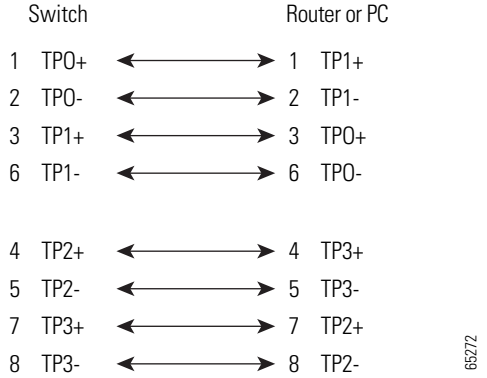
The following figures show these schematics:

- Two twisted-pair, straight-through cable
- Four twisted-pair, straight-through cable

Two Twisted-pair Straight-through Cable Schematic



Four Twisted-pair Straight-through Cable Schematic



When connecting the ports to 10BASE-T- and 100BASE-TX-compatible devices, such as switches or repeaters, you can use a two or four twisted-pair, crossover cable.

The following figures show these schematics:

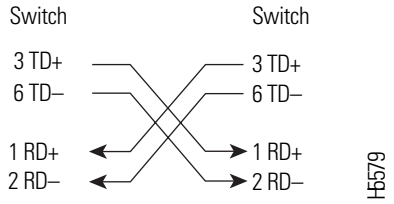
- Two twisted-pair, crossover cable schematics
- Four twisted-pair, crossover cable schematics

Use a straight-through cable to connect two ports only when one port is designated with an X. Use a crossover cable to connect two ports when both ports are designated with an X or when both ports do not have an X.

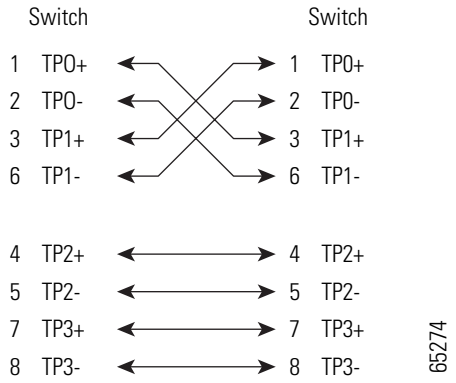
You can use Category 3, 4, or 5 cabling when connecting to 10BASE-T-compatible devices. You must use Category 5 cabling when connecting to 100BASE-TX-compatible devices.

IMPORTANT Use a four twisted-pair, Category 5 cable when connecting to a 1000BASE-T-compatible device

Two Twisted-pair Crossover Cable Schematic



Four Twisted-pair Crossover Cable Schematic

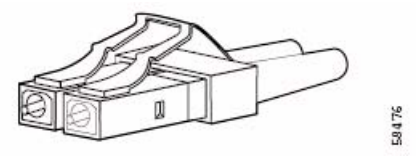


100BASE-FX Ports

The 100BASE-FX ports use the following:

- LC connectors, as shown in the following figure.
- 50/125- or 62.5/125-micron multimode fiber-optic cables

Fiber-optic SFP Module LC Connector



ATTENTION

Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

SFP Module Ports

The switch uses SFP modules for fiber-optic uplink ports.

ATTENTION

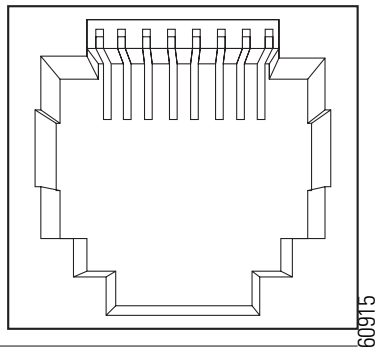
Invisible laser radiation may be emitted from disconnected fibers or connectors. Do not stare into beams or view directly with optical instruments.

Dual-purpose Ports

The Ethernet port on a dual-purpose port uses standard RJ45 connectors. The following figure shows the pinouts.

Ethernet Port RJ45 Connector

Pin	Label
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



The SFP module slot on a dual-purpose port uses SFP modules for fiber-optic ports.

IMPORTANT The auto-MDIX feature is enabled by default. For configuration information for this feature, see the switch software configuration guide or the switch command reference.

Console Port

The console port uses an 8-pin RJ45 connector. The supplied RJ45-to-DB-9 adapter cable is used to connect the console port of the switch to a console personal computer. You need to provide an RJ45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal.

Cable and Adapter Specifications

These sections describe the cables and adapters used with the switches.

SFP Module Cable Specifications

The following lists the cable specifications for the rugged fiber-optic SFP module connections. Each port must match the wave-length specifications on the other end of the cable, and for reliable communication, the cable must not exceed the rated maximum cable length.

Fiber-optic SFP Module Port Cabling Specifications

SFP Module Type	Cat. No.	Wavelength (nm)	Fiber Type	Core Size/Cladding Size (micron)	Modal Bandwidth (MHz/km)[1]	Cable Distance
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62.5/125	500 500	2 km (6562 ft) 2 km (6562 ft)
100BASE-LX	1783-SFP100LX	1310	SMF	G.652[2]	—	10 km (32,810 ft)
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125 62.5/125 50/125 50/125	160 200 400 500	220 m (722 ft) 275 m (902 ft)) 500 m (1640 ft) 550 m (1804 ft)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652[2]	—	10 km (32,810 ft)

(1) Modal bandwidth applies only to multimode fiber.

Adapter Pinouts

The following table lists the pinouts for the console port, the RJ45-to-DB-9 adapter cable, and the console device.

Switch Console Port (DTE)	RJ45-to-DB-9 Terminal Adapter	Console Device
Signal	**DB-9 Pin**	**Signal**
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

The following table lists the pinouts for the console port, RJ45-to-DB-25 female DTE adapter, and the console device.

The RJ45-to-DB-25 female DTE adapter is not supplied with the switch.

Switch Console Port (DTE) Signal	RJ45-to-DB-25 Terminal Adapter DB-25 Pin	Console Device Signal
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

Notes:

A

adapter pinouts, terminal
- RJ45-to-DB-25 164
- RJ45-to-DB-9 164

additional resources 10
address aliasing 35
Alert Log 102
- using 102

allocation, memory 17
announce interval 86
announce receipt timeout interval 86
auto-MDIX 159, 163
- default 65
- setting 65

autonegotiation
- duplex mode 65
- speed 65
- troubleshooting 145

B

bandwidth used gauge 95
boundary mode 83
- timing message settings 85

broadcast storms 36

C

cables
- crossover
  - four twisted-pair pinout, 1000BASE-T ports 161
  - identifying 160
  - using 160
- optical 164
- SFP module 164
- straight-through
  - two twisted-pair pinout 160
  - using 160

cabling
- auto-MDIX 159, 163

CIP
- data 112

CIP network connections 110
CIP VLAN 21, 68
clock
- parent 83
- synchronization 84

connection
- troubleshooting
  - direct managed mode 146

connectors and cables
- 10/100/1000 160, 161
- console 163, 165
- dual-purpose 163
- SC connectors 162
- SFP module ports 162

console port
- specifications 163, 165

crossover cable
- pinout
  - four twisted-pair, 1000BASE-T ports 161

cryptographic software
- SSL 47

customization
- CIP VLAN 21, 68
- default gateway 20, 68
- DHCP persistence 80
- DHCP server 76
- IP address 19, 21, 67, 68
  - DHCP IP address pool 79
  - switch port 82
- IP address (for connected devices) 76, 80
- IP address (switch port) 80
- IP assignment mode 19, 67
- management interface (VLAN ID) 19, 67
- management VLAN 19, 67
- Smartports port roles 29
- subnet mask 19, 67
  - CIP VLAN 21, 68

D

data types
- I/O 151

default gateway
- customization 20, 68

default router 79
default VLAN 31, 63
delay request interval 87
denial-of-service attack 36
device manager 22
- overview 22
- troubleshooting 144
  - display 144
  - no network access 144
  - operating improperly 144

DHCP
- IP assignment mode 19, 67
- troubleshooting 143

DHCP IP address pool
- creating 78
- deleting 78
- modifying 78

DHCP persistence 80
DHCP Pool Name 79
DHCP Pool Network 79
DHCP server 41
diagnostics
link test 142
report 143
switch test 141
direct managed mode
accessing 146
DNS server1 and 2 79
domain name 79
dual-purpose ports
connectors and cables 163
duplex
troubleshooting 145
duplex mode
default 65
setting 65

E

end-to-end transparent mode 83
EtherChannels
creating 75
deleting 75
maximum number supported 75
modes
LACP 75
Port Aggregation Protocol 75
Static 75
modifying 75
Ethernet Industrial Protocol 104
See Ethernet/IP
Ethernet/IP Protocol 30, 104, 125
Express Setup 17

F

features
device manager 22
firmware upgrade, troubleshooting 150
full-duplex mode 65

H

half-duplex mode 65

I

I/O data types 151
IEEE 802.3ad (LACP) mode 75
IGMP snooping
and address aliasing 35
changing 71
definition 34
features 71
initial setup mode 66, 68
input tags 151
IP address
CIP VLAN
assigning 21, 68
modifying 21, 68
customization 19, 67
CIP VLAN 21, 68
DHCP IP address pool 79
switch port 82
customization (connected devices) 76
customization (switch port) 80
DHCP IP address pool
ending range 79
starting range 79
IP assignment mode 19, 67
switch port 82
assigning 82
deleting 82
modifying 82
troubleshooting 143
DHCP 143
wrong IP address 143
IP assignment mode
customization 19, 67
default 19, 67
DHCP 19, 67
Static 19, 67

L

LACP mode, EtherChannels 75
LC connector 162
lease length 79
link integrity, verifying with REP 46
log
See Alert Log

M

management interface 22
customization 19, 67
See also device manager
management VLAN 31
changing 19, 67
customization 19, 67
memory 17
MIBs, supported 48

mismatch prevention, Smartports port roles 31
modes, management
direct managed 146
initial setup 66, 68
monitoring
Alert Log 102
bandwidth used gauge 95
network analyzer 49
packet error gauge 96
port error graph 97
port mirroring 49
port utilization graph 97
status field 61
switch information 95
temperature status 97
trends
overview 98
why use 98
multicast storm 36

O

output tags 151
Overview tab, Dashboard 101

P

packet error gauge 96
parent clock 83
pinouts
10/100 ports 162
crossover cables
four twisted-pair, 1000BASE-T ports 161
RJ45-to-DB-25 terminal adapter 165
RJ45-to-DB-9 terminal adapter 164
SFP module 162
straight-through cables
two twisted-pair 160
pool name 82
pop-up blockers 23, 147
Port Aggregation Protocol
See PAgP
port error graph 97
port numbering 64
port security
violations 39
port settings
auto-MDIX 65
description 64
descriptions of 64
duplex mode 65
enable/disable 64
default 64
speed 65
default 65
Port Type 89
port utilization graph 97
proxy settings 23, 147
PTP
boundary mode 83
timing message settings 85
end-to-end transparent mode 83
synchronization clock mode 84

R

Receive Detail tab, Dashboard 102
recovery
firmware upgrade 150
switch software 149
redundancy
EtherChannel 41
REP 42
open segment 43
ring segment 44
segments
characteristics 45
verifying link integrity 46
REP Admin VLAN 88
REP segments 42
configure 88
reset, troubleshooting 148
residence time 83
RJ45 connector, console port 163
RSLinx software 111
RSTP
changing 71
features 71
RSWho 111

S

SC connector 162
Segment ID 88
segment topology change notices
See also STCNs 89
set up the switch 17
SFP modules
cables 164
connectors 162
Smartports port roles
applying 62

changing VLAN memberships 63
customization 63
optimize ports 29
mismatch prevention 31
SNMP
configuring 72
default 72
MIBs supported 48
snooping, IGMP 34
software features
customization
DHCP persistence settings 80
DHCP server settings 76
Smartports port roles 29
troubleshooting
firmware upgrade 106
Spanning Tree Protocol 42
See also Rapid Spanning Tree Protocol
speed
troubleshooting 145
speed, setting 65
Static mode, EtherChannels 75
Static mode, Port Aggregation Protocol 75
STCN Interface 89
STCN Segment 89
STCN STP 89
storm control
described 36
thresholds 37
straight-through cable
pinout
two twisted-pair 10/100 ports 160, 161
subnet mask
customization 19, 67
CIP VLAN 21, 68
DHCP IP address pool 79
switch
configuration
DHCP persistence settings 80
DHCP server settings 76
management
device manager 22
monitoring
Alert Log 102
network analyzer 49
port mirroring 49
troubleshooting 141
device manager display 144
device manager not accessible 144
device manager problems 144
DHCP 143
direct managed mode 146
firmware upgrade 150
IP address problems 143
reset switch 148
switch software 149
wrong IP address 143
switch software, troubleshooting 149
switch, setup 17
sync interval 87
sync limit 87
synchronization clock mode
boundary 83, 85
end-to-end transparent 83
setting 84

T

tags
input 151
output 151
temperature
status 97
threshold, traffic level 37
timing message settings, PTP boundary mode 85
traffic suppression 37
Transmit Detail tab, Dashboard 102
trends
overview 98
why use 98
troubleshooting 141
device manager display 144
device manager not accessible 144
device manager problems 144
DHCP 143
direct managed mode 146
firmware upgrade 106, 150
IP address problems 143
reset switch 148
speed, duplex, and autonegotiation 145
switch performance 144
switch software 149
wrong IP address 143

U

unicast storm 36
upgrade firmware 106

V

View list 60

VLAN memberships
changing 63
prerequisite 63
VLANs
advanced settings 71
default VLAN 31
grouping different users 34
isolating traffic 33
management VLAN 31
maximum number supported 70

W

WINS server1 and 2 79

Rockwell Automation Support

Rockwell Automation provides technical information on the Web to assist you in using its products. At http://www.rockwellautomation.com/support/, you can find technical manuals, a knowledge base of FAQs, technical and application notes, sample code and links to software service packs, and a MySupport feature that you can customize to make the best use of these tools.

For an additional level of technical phone support for installation, configuration, and troubleshooting, we offer TechConnect support programs. For more information, contact your local distributor or Rockwell Automation representative, or visit http://www.rockwellautomation.com/support/.

Installation Assistance

If you experience an anomoly within the first 24 hours of installation, review the information that is contained in this manual. You can contact Customer Support for initial help in getting your product up and running.

United States or Canada	1.440.646.3434
Outside United States or Canada	Use the Worldwide Locator at http://www.rockwellautomation.com/support/americas/phone_en.html, or contact your local Rockwell Automation representative.

New Product Satisfaction Return

Rockwell Automation tests all of its products to ensure that they are fully operational when shipped from the manufacturing facility. However, if your product is not functioning and needs to be returned, follow these procedures.

United States	Contact your distributor. You must provide a Customer Support case number (call the phone number above to obtain one) to your distributor to complete the return process.
Outside United States	Please contact your local Rockwell Automation representative for the return procedure.

Documentation Feedback

Your comments will help us serve your documentation needs better. If you have any suggestions on how to improve this document, complete this form, publication RA-DU002, available at http://www.rockwellautomation.com/literature/.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Brussels, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication 1783-UM003D-EN-E - December 2009
Supersedes Publication 1783-UM003C-EN-E - June 2009
Copyright © 2009 Rockwell Automation, Inc. All rights reserved. Printed in the U.S.A.